Contact Committee

Comitato di contatto

delle Istituzioni superiori di controllo dell'UE

Compendio di audit

La cibersicurezza nell'UE e nei suoi Stati membri

Audit sulla resilienza delle infrastrutture digitali e dei sistemi informativi critici ai ciberattacchi

Relazioni di audit
pubblicate nel periodo 2014-2020

IT

Dicembre 2020

Il comitato di contatto delle istituzioni superiori di controllo (ISC) dell'Unione europea (UE) rappresenta un forum in cui discutere e affrontare questioni relative all'audit del settore pubblico dell'UE. Intensificando il dialogo e la cooperazione fra i propri membri, il comitato contribuisce a rendere più efficace l'audit esterno delle politiche e dei programmi dell'UE, nonché a promuovere la rendicontabilità, a migliorare la gestione finanziaria dell'UE e a consolidare la buona governance, a beneficio di tutti i cittadini dell'Unione.

Indirizzo di contatto: www.contactcommittee.eu

Indice

Indice

Indice

Prefazione

Cari lettori,

la digitalizzazione e il crescente uso delle tecnologie dell'informazione in tutti gli aspetti della nostra vita quotidiana aprono davanti a noi un nuovo mondo di opportunità. Al contempo, però, aumentano il rischio che singoli cittadini, imprese e autorità pubbliche cadano vittima della cibercriminalità o di ciberattacchi e l'impatto economico e sociale da questi prodotto.

Nell'UE, la cibersicurezza è prerogativa degli Stati membri. L'UE ha il compito di istituire un quadro normativo comune nell'ambito del mercato unico dell'UE e di creare condizioni che consentano agli Stati membri di collaborare in un clima di fiducia reciproca.

La cibersicurezza e la nostra autonomia digitale sono diventate un tema di importanza strategica per l'UE e gli Stati membri. Benché a livelli diversi, in tutti gli Stati membri permangono debolezze nella governance della cibersicurezza nel settore pubblico e privato, che compromettono la nostra capacità di limitare i ciberattacchi e, se necessario, di rispondervi. La disinformazione, spesso orchestrata dall'esterno dell'UE, si sta diffondendo, come avvenuto ancora una volta quest'anno durante l'epidemia di COVID-19. Si tratta di una minaccia, che non possiamo ignorare, per la coesione delle nostre società e per la fiducia dei cittadini nei nostri sistemi democratici.

Nel 2018 un'indagine condotta presso le istituzioni superiori di controllo (ISC) dell'UE ha indicato che fino a quel momento circa la metà di esse non aveva effettuato audit nel campo della cibersicurezza. Da allora queste ISC hanno concentrato maggiormente i propri lavori di audit sulla cibersicurezza, dedicando particolare attenzione alla protezione dei dati, alla preparazione dei sistemi a reagire ai ciberattacchi e alla protezione dei sistemi dei servizi essenziali di pubblica utilità. Come ben si comprende, non è possibile rendere pubblici tutti questi audit, poiché alcuni possono riguardare informazioni sensibili (per la sicurezza nazionale).

Nel corso di quest'anno, la crisi della COVID-19 ha messo alla prova il tessuto economico e sociale delle nostre società. Considerata la nostra dipendenza dalle tecnologie dell'informazione, la prossima pandemia potrebbe assumere la forma di una "crisi cibernetica". Dobbiamo prepararci e accrescere la resilienza delle infrastrutture digitali e dei sistemi informativi critici ai ciberattacchi.

Ci auguriamo che la panoramica offerta in questo compendio stimoli ulteriormente l'interesse degli auditor pubblici di tutta l'Unione per questo settore cruciale.

Klaus-Heiner Lehne

Presidente della Corte dei conti europea
Presidente del Comitato di contatto
e leader del progetto

Sintesi

I La cibersicurezza e la nostra autonomia digitale sono diventate un **tema di importanza strategica per l'UE e i suoi Stati membri** e, man mano che il livello della minaccia cresce, occorre intensificare gli sforzi per proteggere le infrastrutture digitali e i sistemi informativi critici dai ciberattacchi. La cibersicurezza non riguarda soltanto i servizi di pubblica utilità, la difesa o i sistemi sanitari; tocca anche la protezione dei dati personali, i modelli aziendali e la proprietà intellettuale. In ultima analisi, la cibersicurezza riguarda la protezione delle nostre società democratiche, della nostra indipendenza di europei e del modo in cui conviviamo.

II La prima sezione di questo terzo compendio a cura del comitato di contatto descrive **cosa sia la cibersicurezza e le sue implicazioni.** Mostra come questa rappresenti una sfida per le autorità pubbliche, le imprese e i singoli cittadini; mette poi in rilievo il nuovo fenomeno della disinformazione, che costituisce una minaccia sempre più grave per la coesione delle nostre società e per i nostri sistemi democratici. Illustra inoltre quali sono le competenze e gli attori in materia di cibersicurezza dell'UE, la strategia e la legislazione nonché i finanziamenti europei disponibili in questo campo.

III La seconda parte del compendio riassume **i risultati di una selezione di audit effettuati dalle dodici istituzioni superiori di controllo degli Stati membri che hanno contribuito al presente compendio e dalla Corte dei conti europea**; gli audit sono stati pubblicati fra il 2014 e il 2020. Questi audit hanno affrontato importanti aspetti della cibersicurezza, come la protezione dei dati privati, l'integrità dei centri dati nazionali, la sicurezza degli impianti dei servizi di pubblica utilità, nonché l'attuazione delle strategie nazionali di cibersicurezza in senso lato.

IV La terza parte del compendio contiene **dettagliate schede informative relative agli audit selezionati**, insieme a una sintesi di altri audit riguardanti il tema della cibersicurezza pubblicati dalle ISC.

PARTE I – La cibersicurezza nel contesto europeo

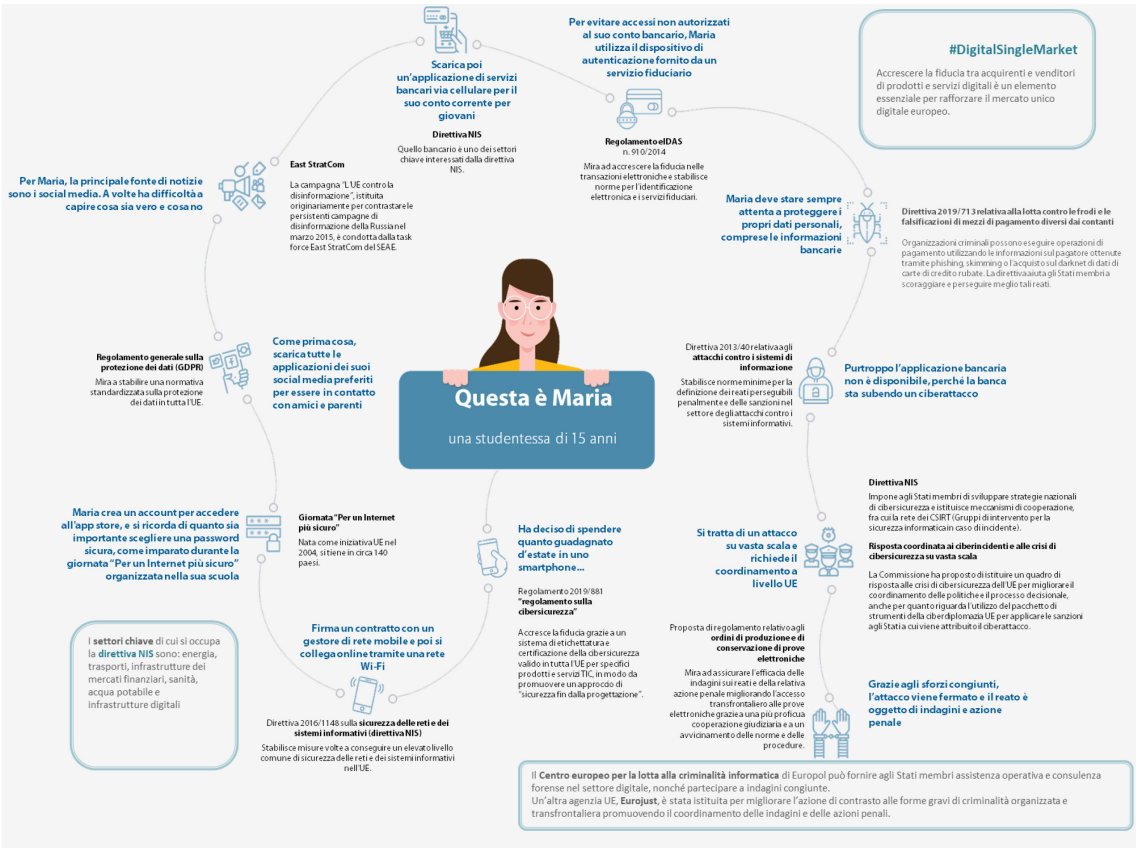
Che cos'è la cibersicurezza?

1 Non esiste una **definizione di cibersicurezza** convenzionale e universale. Nel presente documento, il termine cibersicurezza si riferisce alle **attività necessarie per tutelare i sistemi di rete e di informazione, i loro utenti e le altre persone colpite da minacce informatiche**. Include la prevenzione e l'individuazione dei ciberincidenti, la risposta agli stessi e il successivo recupero. Tali incidenti possono essere intenzionali o non intenzionali e vanno dalla divulgazione accidentale di informazioni agli attacchi a imprese e a infrastrutture critiche, dal furto di dati personali fino addirittura alle ingerenze nei processi democratici e nelle elezioni, o ancora a campagne generali di disinformazione tese a influenzare i dibattiti pubblici.

La cibersicurezza riguarda la vita quotidiana di tutti i cittadini dell'UE

2 La cibersicurezza incide sulla vita quotidiana di tutti i cittadini dell'UE, ogni volta che usano dispositivi informatici personali come smartphone, reti WIFI, social media o servizi bancari elettronici. Nel 2020, come mai prima d'ora, la questione non è più se si verificheranno ciberattacchi, ma come e quando avverranno. Queste minacce riguardano tutti: **singoli cittadini, imprese e autorità pubbliche.** L'***immagine 1*** illustra in che modo l'UE promuove la cibersicurezza e ha creato un quadro per proteggere le attività elettroniche quotidiane dei cittadini dai ciberattacchi. La protezione delle infrastrutture digitali e dei sistemi informativi critici dai ciberattacchi è diventata una sfida strategica.

Immagine 1 – L'UE promuove la cibersicurezza nella vita quotidiana dei cittadini dell'Unione



Fonte: Corte dei conti europea, pittogrammi realizzati da Pixel perfect e disponibili su www.flaticon.com.

Esistono diversi tipi di minacce alla cibersicurezza

3 I numerosi tipi di minacce alla cibersicurezza che gravano sulle nostre società possono essere classificati in base a **ciò che comportano per i dati – divulgazione, modifica, distruzione o rifiuto di accesso** – oppure ai princìpi fondamentali di sicurezza delle informazioni che vengono violati (cfr. ***figura 1***).

Figura 1 – Tipi di minacce e principi di sicurezza delle informazioni da queste messi a rischio

Lucchetto = nessun impatto per la sicurezza; punto esclamativo = sicurezza a rischio

Fonte: Corte dei conti europea, sulla base di uno studio del Parlamento europeo[1].

4 Ogni volta che un dispositivo si connette online o si collega ad altri dispositivi, aumenta la cosiddetta "superficie d'attacco" alla cibersicurezza. La crescita esponenziale dell'Internet delle cose (Internet of Things, IoT), del cloud, dei megadati e della digitalizzazione dell'industria è accompagnata da un aumento dell'esposizione delle vulnerabilità, che consente agli autori degli attacchi di mirare a un numero sempre maggiore di vittime. È difficile stare al passo con tipi di attacco così vari e sempre più sofisticati[2]. Il ***riquadro 1*** descrive esempi di **possibili ciberattacchi**.

[1] Parlamento europeo, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, studio per la commissione LIBE, settembre 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017*, 18 gennaio 2018.

Riquadro 1

Tipi di ciberattacchi

Un **malware** (software malevolo) è concepito per danneggiare dispositivi o reti. Può comprendere virus, trojan, ransomware, worm, adware e spyware (ad esempio, NotPetya).

Un **ransomware** crittografa i dati, impedendo agli utenti di accedere ai propri file finché non pagano un riscatto, generalmente in una criptovaluta, o finché non eseguono un'azione. Secondo Europol, gli attacchi con ransomware sono quelli più diffusi e il numero di tipi di ransomware è esploso negli anni recenti (ad esempio, WannaCry[3])

Aumentano anche gli attacchi **distribuiti di negazione del servizio** (*Distributed Denial of Service*, DDoS), che mettono fuori uso servizi o risorse inondandoli con più richieste di quante siano in grado di gestire; nel 2017 un terzo delle organizzazioni ha subito questo tipo di attacco[4].

Gli **attacchi via web** rappresentano uno dei metodi preferiti per ingannare le vittime utilizzando sistemi e servizi web come vettori della minaccia. Questi prendono di mira una vasta superficie d'attacco: ad esempio, utilizzano URL o script malevoli che indirizzano l'utente o la vittima verso il sito web desiderato, oppure scaricano contenuti nocivi (attacchi watering hole, attacchi drive-by) e **inseriscono** un codice malevolo in un sito web legittimo, ma compromesso, per sottrarre informazioni (formjacking) per ottenere un utile finanziario o sottrarre informazioni[5].

Gli utenti possono essere indotti a eseguire inconsapevolmente un'azione o a divulgare informazioni riservate. Questo stratagemma, noto come **ingegneria sociale**, può essere usato per il furto di dati o ciberspionaggio. Vi sono diversi modi per raggiungere tale scopo, ma un metodo diffuso è il **phishing**, in cui e-mail che sembrano provenire da fonti fidate inducono con l'inganno gli utenti a rivelare informazioni o a cliccare su link che infetteranno i dispositivi scaricando malware. Oltre metà degli Stati membri ha segnalato indagini su attacchi in rete di questo tipo[6].

Forse il tipo di minaccia più nefasto è costituito dalle **minacce persistenti avanzate** (APT), ad opera di soggetti sofisticati impegnati in attività di monitoraggio a lungo termine e furto di dati, talvolta con finalità distruttive. Lo scopo è di passare inosservati quanto più a lungo possibile. Le APT sono spesso collegate ad attività di Stato e mirate a settori particolarmente sensibili, quali tecnologia, difesa e infrastrutture critiche. A questo tipo di **ciberspionaggio** si può ascrivere, a quanto sembra, almeno un quarto di tutti i ciberincidenti[7].

L'impatto economico dei ciberattacchi è significativo

5 Negli ultimi anni la minaccia **dei ciberattacchi e della cibercriminalità** è divenuta un grave problema. Già nel 2016, l'80 % delle imprese dell'UE aveva subito almeno un incidente di cibersicurezza[8]. Nel 2018, il 40 % degli intervistati in un'indagine, appartenenti a organizzazioni che impiegano la robotica o l'automazione, ha dichiarato che il danno più grave di un ciberattacco ai loro sistemi sarebbe l'interruzione delle operazioni. Tuttavia, pur essendo consapevoli della portata distruttiva dei ciber-rischi, le aziende raramente dispongono di un sistema per contrastarli[9].

6 Da allora il numero, la gravità e i costi finanziari dei ciberattacchi continuano a crescere. Per quanto sia possibile stimarne l'**impatto finanziario**, la cibercriminalità comporterà per l'economia globale un **costo annuo di 6 000 miliardi di dollari entro il 2021**, rispetto ai 3 000 miliardi di dollari stimati nel 2015[10], e a un PIL globale stimato a 138 000 miliardi di dollari nel 2020. I costi della cibercriminalità comprendono il danneggiamento e la distruzione dei dati, la sottrazione di denaro, la perdita di produttività, il furto di proprietà intellettuale, il furto di dati personali e finanziari, l'interruzione del normale corso delle attività economiche dopo gli attacchi e i danni

---

[3] Il ransomware "WannaCry" ha sfruttato vulnerabilità del protocollo di Microsoft Windows consentendo l'appropriazione a distanza di qualsiasi computer. Una volta scoperta la vulnerabilità, la Microsoft ha diffuso una patch. Ciononostante, siccome centinaia di migliaia di computer non erano stati aggiornati, molti sono stati in seguito infettati. *Fonte:* A. Greenberg, *Hold North Korea Accountable for Wannacry—and the NSA, too*, WIRED, 19 dicembre 2017.

[4] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*.

[5] ENISA, *ENISA Threat Landscape 2020 – Web-based attacks*, 20 ottobre 2020.

[6] Europol, vedi sopra, 2018.

[7] European Centre for International Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper n. 2/18, febbraio 2018.

[8] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2017*.

[9] PWC, Global State of Information Security (GSISS) *Survey – Strengthening digital society against cyber shocks*, 2017.

[10] Cybersecurity Ventures, *2019 Official Annual Cybercrime Report*, sponsorizzato da Herjavec Group, 2019.

reputazionali. Secondo le stime del Comitato europeo per il rischio sistemico (CERS), tra il 2015 e il 2020 il costo medio dei ciberincidenti è aumentato del 72 %[11].

7 Come risulta da un recente studio del 2020[12], la cibercriminalità **colpisce i diversi settori dell'economia con violenza variabile**: ha costituito il tipo di frode più distruttiva per i governi e le pubbliche amministrazioni, per il settore della tecnologia, dei media e delle telecomunicazioni e per il settore sanitario (cfr. ***riquadro 2***); è stata il secondo tipo di frode per capacità distruttiva nel settore finanziario e in quello industriale e manifatturiero.

Riquadro 2

Pazienti di un centro di psicoterapia finlandese ricattati dopo il furto di dati medici personali tra il 2018 e il 2019

Nel 2020 un ricattatore ha contattato individualmente i pazienti di un grande centro di psicoterapia finlandese, con filiali in tutto il paese, dopo aver rubato i loro dati personali nel novembre 2018 e dopo un'altra potenziale violazione nel marzo 2019. Da quanto risulta, i dati sottratti comprendevano estremi di identificazione personale e appunti sui contenuti delle sedute terapeutiche.

Il ricattatore aveva chiesto al centro e ai pazienti il pagamento di un riscatto in bitcoin per non rendere pubblici i dati. L'incidente ha indotto il governo finlandese a tenere una riunione di emergenza[13].

8 Nel 2019 l'Europol[14] ha sottolineato ancora una volta la **persistenza e la tenacia di alcune delle principali minacce lanciate dalla cibercriminalità**:

- gli attacchi di ransomware rimangono la minaccia più grave: vengono mirati in maniera sempre più precisa, sono più redditizi e provocano danni economici maggiori. Fino a quando continueranno a costituire una fonte di reddito relativamente facile per i cibercriminali e a provocare ingenti danni e perdite

[11] CERS, Comitato europeo per il rischio sistemico, *Systemic cyber risk*, febbraio 2020.

[12] PWC, *Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey*, 2020.

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach*, 26 ottobre 2020.

[14] Europol, *INTERNET organised crime threat assessment (IOCTA)*, 2019.

finanziarie, i ransomware rimarranno probabilmente la principale minaccia della cibercriminalità;

- il phishing e i protocolli di desktop remoto (RDP) vulnerabili rappresentano i principali vettori di infezioni primarie di malware e
- i dati continuano ad essere i principali obiettivi della cibercriminalità, come merce e come fattore facilitatore.

9 Analogamente, nella **relazione del 2020 "*Main incidents in the EU and worldwide*"**[15], l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) elenca una serie di esempi di incidenti di cibersicurezza (cfr. ***riquadro 3***).

Riquadro 3

Agenzia dell'Unione europea per la cibersicurezza (ENISA): incidenti di cibersicurezza 2019-2020

La piattaforma di e-mail verifications.io ha subito una grave violazione di dati a causa di una banca dati MongoDB non protetta. Sono stati divulgati i dati di oltre 800 milioni di e-mail, contenenti informazioni sensibili che comprendevano dati di identificazione personale.

Oltre 770 milioni di indirizzi e-mail e 21 milioni di password uniche sono stati divulgati in un popolare forum di hacker ospitato dal servizio cloud MEGA1. Si è trattato della più ingente raccolta di credenziali personali violate in tutta la storia, che è stata denominata "Collection #1".

La società Citrix, fornitrice di servizi di cloud e virtualizzazione, è stata vittima di un ciberattacco mirato. Per riuscire ad accedere ai sistemi di Citrix, i responsabili dell'attacco hanno sfruttato varie vulnerabilità critiche del software, come CVE-2019-19781, e hanno impiegato una tecnica definita "password spraying".

Il fornitore di servizi di cloud hosting iNSYNQ19 ha subito un attacco di ransomware che ha impedito ai clienti di accedere ai propri dati per più di una settimana, obbligandoli ad affidarsi a backup locali.

[15] ENISA, *Main incidents in the EU and worldwide – January 2019 to April 2020*, ottobre 2020.

10 Secondo Europol, nei primi sei mesi del 2019 i ciberattacchi concepiti per provocare **danni duraturi** sono raddoppiati, soprattutto nel settore manifatturiero. A differenza dei convenzionali attacchi di ransomware, si tratta in questo caso di atti di sabotaggio che cancellano definitivamente o danneggiano irreversibilmente i dati dell'impresa (cfr. ***riquadro 4***).

Riquadro 4

Ransomware distruttivo: gli attacchi di "Germanwiper" nel 2019

Nel 2019 è stata identificata una serie di attacchi di ransomware diretti contro imprese operanti in Germania. Denominato *Germanwiper*, questo ransomware ha la capacità di riscrivere i file infetti sostituendoli con una serie di zero e uno, rendendo così impossibile il recupero dei file. Il ransomware si diffonde tramite campagne di e-mail phishing ed è diretto in particolare al personale addetto alle risorse umane delle grandi aziende, essendo contenuto in false candidature a posti di lavoro[16].

La consapevolezza delle minacce alla cibersicurezza cresce di pari passo con l'intensificarsi della loro frequenza

11 Fino a poco tempo fa la conoscenza e la consapevolezza di questi rischi era, nonostante ciò, ancora alquanto modesta. Nel 2017 il 69 % delle imprese dell'UE aveva una comprensione nulla o solo basilare della propria **esposizione alle ciberminacce**[17], e il 60 % non aveva mai stimato le **potenziali perdite finanziarie**[18]. Inoltre, secondo un

[16] Cybersecurity Insiders, *GermanWiper Ransomware attack warning for Germany*, senza data.

[17] Scheda informativa della Commissione europea sulla cibersicurezza "*Factsheet on cybersecurity*", settembre 2017.

[18] Nelle perdite rientrano: mancati introiti; costi per la riparazione dei sistemi danneggiati; potenziali responsabilità per informazioni o beni rubati; incentivi versati per mantenere la clientela; premi assicurativi maggiorati; maggiori costi di protezione (nuovi sistemi, assunzioni, corsi di formazione); potenziale liquidazione di spese per la messa a norma o la composizione di controversie.

sondaggio mondiale del 2018, un terzo delle organizzazioni preferisce pagare il riscatto chiesto dagli hacker piuttosto che investire nella sicurezza delle informazioni[19].

12 L'**Eurobarometro 2020 "*Europeans' attitudes towards cyber security*"**[20] illustra il diffondersi della consapevolezza, e della preoccupazione, tra i cittadini dell'UE:

- gli intervistati che usano Internet sono quelli probabilmente più preoccupati per un eventuale uso improprio dei loro dati personali (46 %), per la sicurezza dei pagamenti online (41 %), per il fatto di non riuscire a ispezionare le merci o a chiedere la consulenza di una persona reale, o ancora di non ricevere i beni o i servizi acquistati online (il 22 % in entrambi i casi);
- oltre i tre quarti (76 %) degli intervistati ritengono che il rischio di cadere vittima della cibercriminalità sia in aumento. Molto inferiore (52 %) è però la percentuale di coloro che pensano di essere in grado di proteggersi adeguatamente da soli contro questa minaccia: tale dato rappresenta una diminuzione di nove punti percentuali dal 2018;
- poco più della metà degli intervistati (52 %) ritiene di essere ben informata sulla cibercriminalità, ma soltanto l'11 % dichiara di sentirsi molto ben informato.

La cibersicurezza è un elemento importante della coesione sociale e della stabilità politica

Una nuova minaccia: cibersicurezza e disinformazione

13 La diffusione su vasta scala di una deliberata e sistematica **disinformazione rappresenta una sfida strategica urgente per le nostre democrazie**[21]. La disinformazione e le notizie false possono potenzialmente spaccare le società,

---

[19] NTT Security, *Risk:Value 2018 Report*.

[20] Commissione europea, *Speciale Eurobarometro 499 – Europeans' attitudes towards cyber security*, gennaio 2020.

[21] Secondo lo studio "*The Global Disinformation Order*" dell'università di Oxford (settembre 2019) negli ultimi due anni il numero di paesi colpiti da campagne di disinformazione è più che raddoppiato, giungendo alla cifra di 70.

seminare diffidenza e persino mettere a rischio la coesione sociale e la fiducia nei processi democratici (cfr. ***riquadro 5***).

Riquadro 5

Disinformazione

La Commissione europea definisce disinformazione un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico[22]. Nel concetto di pregiudizio pubblico possono rientrare il discredito dei processi democratici o le minacce a beni pubblici quali la salute, l'ambiente e la sicurezza.

A differenza dei contenuti illegali (che comprendono l'incitamento all'odio, i contenuti terroristici e la pedopornografia), la disinformazione riguarda contenuti legali. Si interseca quindi con valori fondamentali dell'UE, come la libertà di espressione e la libertà dei media. Secondo la definizione della Commissione, la disinformazione non include la pubblicità ingannevole, gli errori di segnalazione, la satira e la parodia, o notizie e commenti chiaramente identificabili come di parte.

14 Nuove tecnologie e nuovi software permettono un'agevole diffusione della disinformazione, a costi relativamente bassi, tramite i **social media e altri canali online**. La disinformazione si concentra di solito su temi sensibili, atti a polarizzare le opinioni e a suscitare forti reazioni emotive, e quindi a essere condivisi con maggiore probabilità. Fra questi temi citiamo i problemi sanitari (ad esempio, le campagne contro i vaccini), i fenomeni migratori, i cambiamenti climatici o le questioni di giustizia sociale.

Campagne di disinformazione avviate da paesi terzi per influenzare i processi democratici

15 La disinformazione si prefigge di polarizzare il dibattito democratico, creare o inasprire le tensioni all'interno della società e screditare i sistemi elettorali, esercitando un impatto ancor più ampio sul tessuto sociale e la sicurezza in Europa. In ultima analisi, danneggia la libertà di opinione e di espressione. La disinformazione è spesso **promossa da soggetti di paesi terzi**, che cercano di destabilizzare le nostre

[22] Commissione europea, comunicazione *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236.

società e i sistemi democratici. In tale contesto, le campagne di disinformazione su vasta scala possono comportare anche l'intrusione abusiva (hacking) nelle reti. Un esempio in questo senso è dato dalla campagna con cui la Russia ha cercato di influenzare il referendum del Regno Unito sul recesso dall'Unione europea (cfr. ***riquadro 6***).

Riquadro 6

Campagne di disinformazione russe contro i processi decisionali democratici[23]

Verso la metà del 2016 dalla Russia è stata lanciata una campagna per influenzare il voto nel referendum del Regno Unito sul recesso dall'Unione europea, svoltosi a giugno di quell'anno. Un'analisi dei tweet ha rilevato che nelle 48 ore precedenti il voto più di 150 000 account russi hanno twittato sul tema *#Brexit* e hanno postato oltre 45 000 messaggi sul voto. Il giorno del referendum, account russi hanno twittato 1 102 volte con l'hashtag *#ReasonsToLeaveEU*.

16 La lotta alla disinformazione rappresenta una sfida fondamentale, data la necessità di trovare il giusto equilibrio tra sicurezza e diritti e libertà fondamentali, stimolando l'innovazione e un mercato aperto. L'UE ha adottato una serie di misure per **lottare contro la disinformazione**.

- Nel 2015, è stata istituita presso il SEAE la **task force "East StratCom"** per contrastare le campagne di disinformazione condotte dalla Russia[24]. Gli esperti hanno elogiato le attività della task force in materia di promozione delle politiche dell'UE, sostegno ai media indipendenti nei paesi del vicinato europeo e previsione, tracciatura e contrasto della disinformazione[25].

---

[23] Park advisors, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Christina Nemr e William Gangware, 2019.

[24] Conclusioni del Consiglio europeo, documento EUCO 11/15 del 20 marzo 2015. Da allora si sono aggiunte altre due task force, una per i Balcani occidentali e l'altra per il vicinato meridionale.

[25] Una relazione dell'Atlantic Council esortava l'UE ad obbligare tutti gli Stati membri ad inviare esperti nazionali alla task force. Cfr.: D. Fried e A. Polyakova, *Democratic Offence Against Disinformation*, 5 marzo 2018.

- Nel 2018, l'ENISA ha redatto una **comunicazione sul contrasto alla disinformazione online**[26]. Le azioni indicate contribuiscono ad aumentare l'attendibilità dei contenuti e sostengono gli sforzi per accrescere l'alfabetizzazione mediatica e in materia di notizie.

- Il Centro comune di ricerca della Commissione ha elaborato un **codice di buone pratiche per l'autoregolamentazione** volontario, basato su strumenti strategici esistenti, che è stato adottato dalle piattaforme online e dal settore della pubblicità[27].

- È stata istituita una **rete europea indipendente di verificatori** (fact-checkers).

La disinformazione ai tempi della COVID-19 e la risposta dell'UE

17 La disinformazione ha costituito un problema anche nel contesto della **crisi sanitaria della COVID-19**[28] (cfr. ***riquadro 7*** per alcuni esempi in questo senso).

[26] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* aprile 2018.

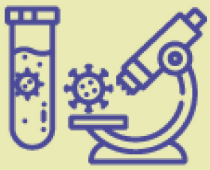
[27] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, aprile 2018.

[28] Reuters Institute e università di Oxford, *Types, Sources, and Claims of Covid-19 Misinformation*, aprile 2020.

Riquadro 7

Esempi di disinformazione relativa alla COVID-19 segnalati dalla Commissione[29]

Affermazioni false, come "bere candeggina o alcol puro può curare le infezioni da coronavirus": queste azioni possono invece essere molto pericolose. **Il centro antiveleni del Belgio ha registrato un aumento del 15 % del numero di incidenti legati all'uso di candeggina.**



Teorie del complotto, ad esempio l'affermazione secondo cui il coronavirus sarebbe "un'infezione causata dalle élite del mondo per ridurre la crescita della popolazione". Le prove scientifiche sono chiare: il virus appartiene a una famiglia di virus che ha origine negli animali e che ne comprende altri, come la SARS e la MERS.

Affermazioni antiscientifiche secondo cui "gli impianti 5G diffondono il virus". Queste teorie sono prive di qualsiasi fondamento e hanno provocato attacchi alle antenne per il 5G.

18 Nel marzo 2020 la Commissione, ENISA, CERT-UE ed Europol hanno pubblicato una **dichiarazione congiunta sulle minacce associate alla COVID-19**[30], in cui rilevavano che soggetti malevoli stavano attivamente sfruttando le difficile circostanze determinate dalla crisi sanitaria pubblica per raggiungere i telelavoratori, le imprese e i singoli cittadini. Inoltre ENISA ha avviato campagne di informazione dedicate ai settori colpiti dalla disinformazione durante la pandemia della COVID-19[31].

---

[29] Commissione europea, *Lotta alla disinformazione sul coronavirus*, senza data.

[30] Dichiarazione congiunta di Commissione europea, ENISA, CERT-UE ed Europol, *Coronavirus outbreak*, 20 marzo 2020.

[31] ENISA, *Schede informative relative alla COVID 19*, 2020.

La verifica dei fatti è fondamentale nella lotta alla disinformazione

19 L'UE ha pure intensificato gli sforzi a sostegno dei verificatori e dei ricercatori europei nel campo della disinformazione. In particolare ha istituito un **Osservatorio europeo dei media digitali** per esaminare e comprendere meglio i fenomeni di disinformazione: attori, vettori, strumenti, metodi, dinamiche di diffusione, obiettivi prioritari e impatto sulla società. Tra gli altri esempi di progetti finanziati dall'UE per affrontare il problema della disinformazione citiamo PROVENANCE, SocialTruth, EUNOMIA e WeVerify.

20 Nel 2018, con il **Codice di buone pratiche sulla disinformazione**[32], l'UE ha proposto, per la prima volta nel mondo, un insieme di norme di autoregolamentazione per la lotta contro la disinformazione. Nell'ottobre 2018 questo codice volontario è stato sottoscritto da piattaforme, importanti reti sociali, inserzionisti e dal settore pubblicitario, come Facebook, Twitter, Mozilla e Google nonché associazioni e membri del settore pubblicitario. Microsoft ha firmato il codice di buone pratiche nel maggio 2019. Tik Tok ha aderito al codice nel giugno 2020.

Garantire la sicurezza delle elezioni del Parlamento europeo del 2019

21 La legittimità dei sistemi democratici europei si basa su un elettorato informato, che esprime la propria volontà democratica tramite **elezioni libere e regolari**. Qualsiasi tentativo malevolo e intenzionale di diffondere sfiducia e manipolare l'opinione pubblica rappresenta perciò una grave minaccia per le nostre società. Le ingerenze nelle elezioni e nelle infrastrutture elettorali potrebbero voler influenzare le preferenze di voto, l'affluenza o il processo elettorale stesso, compresa l'effettiva votazione, lo scrutinio e la comunicazione dei voti. Sulla scia del referendum tenutosi nel Regno Unito, le elezioni europee del 2019 hanno visto per la prima volta un'azione coordinata tra gli Stati membri tesa a **tutelare l'integrità delle elezioni democratiche**: quelle per il Parlamento europeo ma anche quelle per i parlamenti nazionali.

[32] *Codice di buone pratiche dell'UE sulla disinformazione*, settembre 2018.

22 Come indicato in precedenza, nell'aprile 2018 la Commissione ha pubblicato una **comunicazione intitolata "Contrastare la disinformazione online: un approccio europeo"**[33]. La comunicazione è stata seguita, nel settembre 2018, dal **Pacchetto elezioni**[34] concepito per proteggere le elezioni dell'UE e degli Stati membri dalla disinformazione e dai ciberattacchi. Il pacchetto era incentrato sulla protezione dei dati, sulla trasparenza della propaganda politica e dei relativi finanziamenti, sulla cibersicurezza connessa alle elezioni, nonché sulle sanzioni previste per le violazioni delle norme sulla protezione dei dati da parte dei partiti politici. Si è tenuto inoltre un **esercizio congiunto** per verificare l'efficacia delle procedure di risposta e dei piani di crisi dell'UE e degli Stati membri nel proteggere le elezioni del Parlamento europeo (cfr. ***riquadro 8***).

[33] Commissione europea, *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236 final.

[34] Commissione europea, *Stato dell'Unione 2018*, settembre 2018.

Riquadro 8

ELEx19 –Garantire la sicurezza delle elezioni del Parlamento europeo del 2019[35]

L'esercizio ELex19 sulla resilienza delle imminenti elezioni del Parlamento europeo si proponeva di individuare i modi per prevenire, identificare e attenuare gli incidenti di cibersicurezza che avrebbero potuto influenzare le elezioni del 2019.

L'esercizio, che prefigurava diversi scenari di minacce e incidenti basati sull'uso degli strumenti informatici, ha consentito ai partecipanti di:

— acquisire una visione d'insieme sul livello di resilienza (in termini di strategie adottate, competenze e capacità disponibili) dei sistemi elettorali vigenti nell'UE;

— promuovere la cooperazione tra le autorità competenti a livello nazionale (comprese le autorità elettorali e altri organismi e agenzie pertinenti);

— testare i piani per la gestione delle crisi esistenti, nonché le relative procedure per prevenire, identificare e gestire gli attacchi alla cibersicurezza e le minacce ibride (comprese le campagne di disinformazione) e per rispondere a tali attacchi e minacce;

— migliorare la cooperazione transfrontaliera e rafforzare il collegamento con i gruppi di cooperazione impegnati su tali tematiche a livello dell'UE (ad esempio, la rete di cooperazione in materia elettorale, il gruppo di cooperazione NIS, la rete dei CSIRT); e

— individuare tutte le altre potenziali lacune e le opportune misure di attenuazione dei rischi che si sarebbero dovute attuare prima delle elezioni del Parlamento europeo.

A questo esercizio hanno partecipato oltre 80 rappresentanti degli Stati membri dell'UE, assieme a osservatori del Parlamento europeo, della Commissione e dell'Agenzia dell'Unione europea per la cibersicurezza.

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 5 aprile 2019.

23 Infine, nel dicembre 2018, il Consiglio europeo ha adottato un **Piano d'azione contro la disinformazione**[36] per offrire una risposta coordinata e integrare gli sforzi nazionali. Questo piano d'azione comprende azioni specifiche basate su quattro pilastri: migliorare le capacità delle istituzioni dell'Unione di individuare, analizzare e denunciare la disinformazione; potenziare risposte coordinate e comuni alla disinformazione; mobilitare il settore privato nella lotta alla disinformazione; e sostenere azioni di sensibilizzazione e rafforzare la resilienza sociale.

La cibersicurezza nell'UE: competenze, attori, strategie e legislazione

La cibersicurezza è in primo luogo una responsabilità degli Stati membri

24 Nell'UE, la cibersicurezza è in primo luogo una **competenza degli Stati membri**, soprattutto per quanto riguarda la protezione di informazioni sensibili relative alla sicurezza nazionale. Tutti gli Stati membri si sono dotati di una **strategia nazionale per la cibersicurezza** per affrontare i rischi che potrebbero compromettere il conseguimento dei benefici economici e sociali derivanti dal ciberspazio. La capacità e l'impegno in materia di cibersicurezza variano però ancora da uno Stato membro all'altro.

25 L'UE ha il compito di definire un **quadro normativo comune** nell'ambito del mercato unico dell'Unione e creare condizioni che consentano agli Stati membri di cooperare efficacemente in diversi settori d'intervento in cui la cibersicurezza è importante, quali la giustizia e gli affari interni, il mercato unico, i trasporti, la salute pubblica, la politica dei consumatori e la ricerca. In politica estera, la cibersicurezza svolge un ruolo di primo piano nella diplomazia ed è sempre più parte dell'emergente politica di difesa e sicurezza dell'UE.

---

[36] Commissione europea, Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, *Piano d'azione contro la disinformazione*, JOIN(2018) 36 final. Detto piano è incentrato sui seguenti aspetti: migliorare la capacità delle istituzioni dell'UE di individuare, analizzare e denunciare la disinformazione; potenziare risposte coordinate e comuni alla disinformazione; mobilitare il settore privato; sostenere azioni di sensibilizzazione e rafforzare la resilienza sociale.

26 I principali **attori responsabili per la cibersicurezza a livello dell'UE** sono elencati nel ***riquadro 9*** a seguire.

Riquadro 9

I principali soggetti che si occupano di cibersicurezza a livello dell'UE

La **Commissione europea** si prefigge di sviluppare le capacità e la cooperazione in materia di cibersicurezza, rafforzare il ruolo dell'UE quale attore della cibersicurezza e di integrare questo tema nelle altre politiche dell'UE.

Varie agenzie dell'UE coadiuvano la Commissione, in particolare **ENISA**, **EC3** e **CERT-UE**. L'**Agenzia dell'Unione europea per la cibersicurezza** (nota come **ENISA** in ragione della denominazione originaria "*European Network and Information Security Agency*", ovvero Agenzia europea per la sicurezza delle reti e dell'informazione) è essenzialmente un organo consultivo che coadiuva l'elaborazione delle politiche, il potenziamento delle capacità e l'opera di sensibilizzazione. Il **Centro europeo per la lotta alla criminalità informatica (EC3)** presso Europol è stato istituito per rafforzare l'azione di contrasto dell'UE alla criminalità informatica. La Commissione ospita una **squadra di pronto intervento informatico (CERT-UE)** che assiste tutte le istituzioni, gli organismi e le agenzie dell'Unione.

Il **Servizio europeo per l'azione esterna (SEAE)** è a capo della ciberdifesa, della ciberdiplomazia e della comunicazione strategica e ospita centri di analisi e intelligence. L'**Agenzia europea per la difesa (AED)** è preposta allo sviluppo delle capacità di ciberdifesa.

A livello dell'UE gli Stati membri agiscono tramite il **Consiglio**, che dispone di vari organismi di coordinamento e condivisione di informazioni (tra cui il gruppo orizzontale "Questioni riguardanti il ciberspazio"). Il **Parlamento europeo** interviene come colegislatore.

Le **organizzazioni del settore privato**, tra cui gli operatori del settore, gli organismi di governance di Internet e gli ambienti accademici, partecipano e contribuiscono allo sviluppo e all'attuazione delle politiche, ad esempio attraverso un partenariato pubblico-privato contrattuale (**cPPP**).

La ciberstrategia dell'UE: la cibersicurezza rappresenta un tema di notevole rilevanza sin dal 2013

27 La cibersicurezza rappresenta un tema di notevole rilevanza politica almeno dal 2013, quando la Commissione ha adottato la **strategia per la cibersicurezza**[37], che si pone cinque obiettivi principali:

- accrescere la ciber-resilienza;
- ridurre la cibercriminalità;
- sviluppare una politica e capacità di ciberdifesa;
- sviluppare le risorse industriali e tecnologiche per la cibersicurezza;
- creare una politica internazionale sul ciberspazio coerente con i valori costitutivi dell'UE.

Negli anni successivi, il tema della cibersicurezza è stato affrontato anche da altre strategie dell'UE (cfr. ***riquadro 10***).

[37] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1 final, 7 febbraio 2013.

Riquadro 10

Altre strategie dell'UE in materia di cibersicurezza

- L'**Agenda europea sulla sicurezza** (2015), che mirava a migliorare l'azione di contrasto e la risposta giudiziaria alla criminalità informatica, principalmente rinnovando e/o aggiornando le politiche e la normativa esistenti[38].
- La **strategia per il mercato unico digitale** (2015)[39], che si proponeva di migliorare l'accesso ai beni e ai servizi digitali; a tale fine è essenziale migliorare la fiducia, l'inclusione e la sicurezza online.
- La **strategia globale dell'UE** (2016)[40], che delineava una serie di iniziative volte a promuovere il ruolo dell'UE nel mondo, in cui la cibersicurezza e il contrasto della disinformazione tramite la comunicazione strategica costituivano un pilastro fondamentale.

28 Inoltre, nel 2017, la Commissione europea e l' Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno diffuso una **comunicazione congiunta sulla cibersicurezza per l'UE**[41] diretta al Parlamento europeo e al Consiglio in cui invitavano a realizzare strutture più solide ed efficaci per promuovere la cibersicurezza e a rispondere ai ciberattacchi negli Stati membri, ma anche nelle istituzioni, nelle agenzie e negli organismi dell'UE.

---

[38] Commissione europea, *Agenda europea sulla sicurezza*, COM(2015) 185 final del 28 aprile 2015.

[39] Commissione europea, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final del 6 maggio 2015.

[40] SEAE, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, giugno 2016.

[41] Commissione europea e Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, comunicazione congiunta *"Resilienza, deterrenza e difesa:, verso una cibersicurezza forte per l'UE"*, JOIN(2017) 450 final, 13 settembre 2017.

29 Nel luglio 2020 la Commissione europea ha aggiornato l'agenda del 2015 e ha adottato la **strategia dell'UE per l'Unione della sicurezza**[42] per il periodo 2020-2025, che individua nella cibersicurezza una questione di importanza strategica. In questa strategia, la Commissione mette in rilievo soprattutto le cosiddette minacce ibride che combinano ciberattacchi e campagne di disinformazione, in cui soggetti statali e non statali di paesi terzi agiscono di concerto con l'intento di manipolare l'ambiente di informazione e sferrare attacchi alle infrastrutture fondamentali.

La normativa dell'UE in materia di cibersicurezza: la direttiva sulla sicurezza delle reti e dei sistemi informativi, il regolamento generale sulla protezione dei dati (GDPR), il regolamento sulla cibersicurezza e un nuovo meccanismo di sanzioni

30 Quale pilastro della strategia del 2013 per la cibersicurezza, la componente giuridica portante è la **direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)**[43] del 2016, il primo atto giuridico a livello UE sulla cibersicurezza. La direttiva intende conseguire un livello minimo di capacità armonizzate, imponendo agli Stati membri di adottare strategie NIS nazionali nonché di creare punti di contatto unici e gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)[44]. Stabilisce inoltre obblighi di sicurezza e di notifica per gli operatori di servizi essenziali in settori critici e per i fornitori di servizi digitali.

---

[42] Commissione europea, comunicazione *Strategia dell'UE per l'Unione della sicurezza*, COM (2020)605 final, 24 luglio 2020.

[43] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[44] Questi sono integrati in strutture di cooperazione stabilite dalla direttiva, la rete dei CSIRT (una rete costituita dai CSIRT designati dagli Stati membri dell'UE e dalla CERT-UE; l'ENISA ne ospita il segretariato) e nel gruppo di cooperazione (che assiste e facilita la cooperazione strategica e lo scambio di informazioni tra Stati membri; la Commissione ne ospita il segretariato).

31 Gli Stati membri dovevano recepire **la direttiva NIS nel proprio diritto nazionale** entro maggio 2018. Entro novembre 2018 dovevano inoltre indicare i cosiddetti "operatori di servizi essenziali". La Commissione europea è incaricata di riesaminare periodicamente il funzionamento di questa direttiva. Da luglio a ottobre 2020, nel quadro dell'obiettivo strategico fondamentale di creare "un'Europa pronta per l'era digitale" e in linea con gli obiettivi dell'Unione per la sicurezza, la Commissione ha tenuto una consultazione, i cui risultati serviranno per una prima valutazione e per la valutazione d'impatto ex post della direttiva NIS.

32 Parallelamente, dal maggio 2018 è applicato il **regolamento generale sulla protezione dei dati**[45] (GDPR), che era entrato in vigore nel 2016. Il suo obiettivo è proteggere i dati personali dei cittadini europei fissando regole per il trattamento e la divulgazione degli stessi. Esso riconosce alle persone interessate determinati diritti e impone obblighi ai titolari del trattamento dei dati (fornitori di servizi digitali) in merito all'utilizzo e al trasferimento delle informazioni.

33 Inoltre, il **regolamento sulla cibersicurezza**[46] dell'UE introduce per la prima volta un quadro di certificazione della cibersicurezza esteso a tutta l'UE per prodotti, servizi e processi TIC. In tal modo le imprese che operano nell'UE avranno il vantaggio di dover certificare i propri prodotti, processi e servizi TIC una sola volta, vedendo riconoscere i propri certificati in tutta l'UE. Il regolamento UE sulla cibersicurezza ha anche istituito **l'Agenzia dell'Unione europea per la cibersicurezza** (ENISA, che sostituisce la precedente Agenzia europea per la sicurezza delle reti e dell'informazione). Il regolamento conferisce all'Agenzia il mandato di intensificare la cooperazione operativa a livello UE, fornendo agli Stati membri che lo richiedano sostegno per gestire gli incidenti di cibersicurezza e favorendo il coordinamento dell'UE in caso di crisi e ciberattacchi transfrontalieri su vasta scala.

---

[45] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[46] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

34 Infine, nel maggio 2019 il Consiglio ha istituito uno strumento giuridico che consente all'UE di imporre **misure** restrittive mirate **per scoraggiare e contrastare i ciberattacchi** che costituiscono una minaccia esterna per l'UE o i suoi Stati membri[47]. Di conseguenza l'UE ha il potere giuridico di infliggere sanzioni a persone o entità che:

- sono responsabili di ciberattacchi o tentati ciberattacchi; oppure
- forniscono sostegno finanziario, tecnico o materiale per tali attacchi o vi sono altrimenti coinvolti.

Nel luglio 2020 il Consiglio ha utilizzato per la prima volta queste nuove prerogative (cfr. ***riquadro 11***).

Riquadro 11

Fare sul serio – L'UE impone per la prima volta sanzioni contro i ciberattacchi[48]

Nel luglio 2020 il Consiglio ha imposto misure restrittive nei confronti di sei individui e tre entità responsabili di aver compiuto o partecipato a vari ciberattacchi. Fra questi, il tentato ciberattacco ai danni dell'Organizzazione per la proibizione delle armi chimiche e gli attacchi pubblicamente noti come "WannaCry", "NotPetya" e "Operation Cloud Hopper".

Le sanzioni imposte includono il divieto di viaggio e il congelamento dei beni. È fatto inoltre divieto alle persone ed entità dell'UE di mettere fondi a disposizione delle persone ed entità inserite in tale elenco.

---

[47] Decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri.

[48] Decisione (PESC) 2020/1127 del Consiglio, del 30 luglio 2020, che modifica la succitata decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri.

Cibersicurezza e ciberdifesa

35 Negli ultimi anni abbiamo assistito alla crescente militarizzazione [49] e strumentalizzazione offensiva[50] del ciberspazio, che è ormai considerato la quinta zona di confronto bellico in aggiunta a terra, mare, aria e spazio. Nel 2014 è stato adottato un **quadro strategico UE in materia di ciberdifesa**, successivamente aggiornato nel 2018[51]. L'aggiornamento del 2018 individua alcune priorità, fra cui lo sviluppo delle capacità di ciberdifesa, nonché la protezione delle reti di comunicazione e informazione della politica di sicurezza e di difesa comune (PSDC) dell'UE. La ciberdifesa è anche parte del quadro di cooperazione strutturata permanente (PESCO) e della cooperazione UE-NATO.

36 Sono divenuti frequenti i casi in cui il ciberspazio viene utilizzato a fini politici e in cui la cibersicurezza dell'UE e degli Stati membri viene testata e penetrata in modo aggressivo. Queste attività di ciberspionaggio e di hacking - dirette contro governi nazionali, entità politiche e istituzioni dell'UE per estrarre e raccogliere informazioni classificate - fanno sospettare che siano in corso sofisticate operazioni di ciberspionaggio e manipolazione dei dati a danno dell'Unione e degli Stati membri. Il **quadro congiunto per contrastare le minacce ibride** (2016), applicato nell'UE, riguarda le ciberminacce sia per le infrastrutture critiche che per gli utenti privati, evidenziando il fatto che i ciberattacchi possono essere condotti mediante campagne di disinformazione sui social media[52]. Vi si rileva inoltre la necessità di una

---

[49] Centro per gli studi politici europei, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, novembre 2018.

[50] Il malware utilizzato per sferrare l'attacco di ransomware "WannaCry", attribuito alla Corea del Nord da Stati Uniti, Regno Unito e Australia, è stato sviluppato in origine e tesaurizzato dall'Agenzia statunitense per la sicurezza nazionale al fine di sfruttare le vulnerabilità di Windows.
Fonte: A. Greenberg, WIRED, 19 dicembre 2017. All'indomani degli attacchi, Microsoft ha condannato la tesaurizzazione delle vulnerabilità dei software da parte dei governi e ha ribadito la necessità di una Convenzione di Ginevra digitale, che ha sollecitato.

[51] *Quadro strategico dell'UE in materia di ciberdifesa* (aggiornato nel 2018), 14413/18, 19 novembre 2018.

[52] Commissione europea/Servizio europeo per l'azione esterna, *Quadro congiunto per contrastare le minacce ibride – La risposta dell'Unione europea*, JOIN(2016) 18 final, 6 aprile 2016.

sensibilizzazione e di un rafforzamento della cooperazione tra UE e NATO, che ha trovato riscontro nelle dichiarazioni congiunte UE-NATO del 2016 e del 2018[53].

Spesa UE per la cibersicurezza: dispersiva e di modesta entità

Le spesa per la cibersicurezza nell'UE-27 è inferiore a quella degli USA

37 È difficile stimare la spesa pubblica per la cibersicurezza, a causa della natura trasversale e della difficoltà di distinguere le spese per la cibersicurezza da quelle generali del settore informatico[54]. Fatta questa premessa, i dati disponibili sembrano indicare che la **spesa pubblica per la cibersicurezza** nell'UE sia stata finora relativamente modesta se confrontata con quella di altri paesi:

- Nel 2020 i fondi stanziati dal governo federale degli Stati Uniti per la sola cibersicurezza sono ammontati a circa **17,4 miliardi di dollari**[55].
- A titolo di paragone, la Commissione ha stimato che la spesa pubblica per la cibersicurezza oscilli tra **uno e due miliardi di euro** all'anno per tutti gli Stati membri dell'UE (che nell'insieme hanno un PIL paragonabile quello degli USA)[56].
- Secondo le stime, per molti Stati membri la spesa pubblica per la cibersicurezza in percentuale al PIL è pari a **un decimo di quella degli Stati Uniti** o addirittura inferiore[57].

---

[53] Dichiarazione congiunta del Presidente del Consiglio europeo, del Presidente della Commissione europea e del Segretario generale dell'Organizzazione del Trattato del Nord Atlantico, 8 luglio 2016 e 10 luglio 2018.

[54] Commissione europea, COM(2018) 630 final del 12 settembre 2018.

[55] The White House, *Cybersecurity spending fiscal year 2020*.

[56] Commissione europea, documento di lavoro dei servizi della Commissione: *Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027*, SWD(2018) 305 final del 6 giugno 2018.

[57] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, dicembre 2016.

2014-2020: i finanziamenti dell'UE per la cibersicurezza si disperdono in molti strumenti diversi

38 Secondo la Commissione[58], nel bilancio generale dell'UE vi sono almeno **dieci strumenti differenti** per finanziare iniziative in materia di cibersicurezza (per i programmi più importanti in termini finanziari cfr. ***riquadro 12***). Nel periodo 2014-2020 i finanziamenti totali dell'UE destinati alla cibersicurezza non militare sono ammontati a **meno di 200 milioni di euro all'anno**. Non esiste neppure uno strumento di finanziamento esteso a tutta l'UE che aiuti gli Stati membri a coordinare le proprie attività in materia di cibersicurezza.

[58] Commissione europea, *Impact assessment accompanying the proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*, SWD(2018) 403 final, 12 settembre 2018.

Riquadro 12

Programmi dell'UE a sostegno dei progetti di cibersicurezza (2014-2020)

- Il **programma di ricerca dell'UE Orizzonte 2020** ha assegnato circa 600 milioni di euro a progetti sulla cibersicurezza e cibercriminalità per il periodo 2014-2020. Tale importo include 450 milioni di euro destinati al cPPP ("partenariato pubblico-privato contrattuale") sulla cibersicurezza per il periodo 2017-2020, allo scopo di attrarre altri 1,8 miliardi di euro dal settore privato.

- I **Fondi strutturali e d'investimento europei (fondi SIE)** forniscono un contributo che può giungere a 400 milioni di euro per gli investimenti degli Stati membri nel campo della cibersicurezza fino alla fine del 2020.

- Il **meccanismo per collegare l'Europa (MCE)** ha finanziato investimenti per circa 30 milioni di euro all'anno. Rientra in questo quadro il cofinanziamento di circa 13 milioni di euro all'anno, tra il 2016 e il 2018, per le squadre di pronto intervento informatico (CERT) che gli Stati membri devono istituire ai sensi della direttiva NIS[59].

- Il **Fondo sicurezza interna – Polizia (ISF-Polizia)** finanzia studi, riunioni di esperti e attività di comunicazione; tale sostegno è ammontato a quasi 62 milioni di euro tra il 2014 e il 2017. Gli Stati membri possono anche ricevere, in modalità di gestione concorrente, sovvenzioni per attrezzature, formazione, ricerca e raccolta dati. 19 Stati membri hanno beneficiato di queste sovvenzioni, per un valore di 42 milioni di euro.

- Il **programma Giustizia** ha erogato 9 milioni di euro per sostenere la cooperazione giudiziaria e i trattati di mutua assistenza giudiziaria, con particolare riguardo allo scambio di dati elettronici e di informazioni finanziarie.

[59] Articolo 9, paragrafo 2, della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (la "direttiva NIS").

39 Inoltre, nel 2019 e 2020 sono stati assegnati 500 milioni di euro a titolo del bilancio dell'UE per il **programma europeo di sviluppo del settore industriale della difesa**[60]. incentrato sul miglioramento del coordinamento e dell'efficienza della spesa per la difesa degli Stati membri tramite incentivi per lo sviluppo congiunto. Questo programma mira a generare investimenti, per un totale di 13 miliardi di euro, nelle capacità di difesa dopo il 2020 tramite il Fondo europeo per la difesa, alcuni dei quali riguarderanno la ciberdifesa. Infine, nell'ambito dell'**Iniziativa per la sicurezza europea**, la Banca europea per gli investimenti erogherà, tra il 2018 e il 2020, 6 miliardi di euro in finanziamenti a duplice uso (ricerca e sviluppo/cibersicurezza e sicurezza civile)[61].

2021-2027: il nuovo programma Europa digitale

40 Nelle conclusioni del luglio 2020 sul nuovo quadro finanziario pluriennale (QFP) per il periodo 2021-2027, il Consiglio ha deciso che il **programma Europa digitale**[62] avrebbe investito nelle più importanti capacità digitali strategiche, come il calcolo ad alte prestazioni, l'intelligenza artificiale e la cibersicurezza dell'UE. Il programma sarà complementare ad altri strumenti, in particolare Orizzonte Europa e il meccanismo per collegare l'Europa, nel favorire la trasformazione digitale del nostro continente.

41 Il Consiglio ha deciso inoltre di assegnare 6,8 miliardi di euro al programma Europa digitale per il periodo 2021-2027, ossia circa **970 milioni di euro all'anno.** Si tratta di un considerevole aumento rispetto al periodo 2014-2020, ma di una cifra ancora inferiore a quella inizialmente proposta dalla Commissione (8,2 miliardi di euro per lo stesso periodo, con 2 miliardi di euro destinati al potenziamento del settore della cibersicurezza dell'UE e della protezione sociale generale, sostenendo per esempio l'attuazione della direttiva NIS).

---

[60] Commissione europea, Regolamento (UE) 2018/1092 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che istituisce il programma europeo di sviluppo del settore industriale della difesa, volto a sostenere la competitività e la capacità di innovazione dell'industria della difesa dell'Unione (GU L 200 del 7.8.2018, pag. 30).

[61] Banca europea per gli investimenti; *The EIB Group Operating Framework and Operational Plan 2018*, 12.12.2017.

[62] Commissione europea, *Europe investing in digital: the Digital Europe Programme*, settembre 2020.

PARTE II – Riepilogo delle attività svolte dalle ISC

Introduzione

42 La cibersicurezza e la nostra autonomia digitale sono diventate un tema di importanza strategica per l'UE e gli Stati membri che ne fanno parte. Benché a livelli diversi, la governance della cibersicurezza continua a presentare debolezze nel settore pubblico e privato di tutti gli Stati membri. Questa situazione compromette la nostra capacità di limitare i ciberattacchi e, ove necessario, di rispondervi.

43 Nel 2018, tuttavia, da un'indagine svolta presso le istituzioni superiori di controllo (ISC) dell'UE, è emerso che circa la metà di esse non aveva mai effettuato audit nel settore della cibersicurezza. Da allora le ISC hanno potenziato il proprio lavoro di audit relativo alla cibersicurezza, dedicando particolare attenzione alla protezione dei dati, alla prontezza di reazione del sistema ai ciberattacchi e alla protezione dei sistemi dei servizi pubblici essenziali. Hanno inoltre esaminato altri aspetti di grande importanza. Comprensibilmente, non è possibile rendere pubblici tutti questi audit, poiché alcuni possono riguardare informazioni sensibili (inerenti alla sicurezza nazionale).

44 Data l'importanza della cibersicurezza per il funzionamento delle nostre società e istituzioni politiche, il Comitato di contatto ha deciso di dedicare a tale argomento il compendio di audit di quest'anno. In questa sezione si riassumono i risultati di audit selezionati nel settore della cibersicurezza effettuati dalle ISC di 12 Stati membri e dalla Corte dei conti europea. Ciascuna ISC partecipante ha contribuito con una relazione di audit selezionata, ulteriormente sintetizzata nella parte III. Come si evince dalle ulteriori relazioni indicate dalle ISC partecipanti, sono stati espletati molti altri audit sul tema.

Metodologia degli audit e temi trattati

45 Per quanto riguarda il tipo di audit espletati ai fini delle relazioni sintetizzate nel presente compendio, gran parte delle ISC partecipanti ha effettuato controlli di gestione su temi riguardanti la cibersicurezza, mentre due (Polonia e Ungheria) hanno svolto audit di conformità e uno (la Corte dei conti europea) ha compiuto un'analisi delle politiche.

46 Nel determinare l'approccio di audit, la maggior parte delle ISC ha concepito i propri audit in modo da includervi almeno due modi di valutare l'oggetto dell'audit. Poteva trattarsi di un esame di documenti strategici di alto livello (per esempio, nazionali) o di politiche stabilite, di un'analisi delle procedure intesa a valutarne la conformità alla metodologia COBIT stabilita (cfr. ***riquadro 13***) o ancora di un esame dell'efficacia dei sistemi di gestione informatica in uso. Una ISC (la Corte dei conti dei Paesi Bassi) ha persino fatto ricorso a hacker etici per testare l'efficacia dei sistemi di cibersicurezza utilizzati nell'ambito dei controlli alle frontiere e delle strutture idriche critiche. Nel ***riquadro 14*** sono sintetizzati schematicamente i metodi e le tecniche utilizzati dalle varie ISC per condurre il proprio lavoro di audit.

Riquadro 13

Cosa si intende per COBIT?

COBIT (*Control Objectives for Information and Related Technology*, obiettivi di controllo nel campo dell'informazione e delle tecnologie correlate) è un quadro di migliori pratiche e procedure riconosciute per la gestione e la governance informatiche, definito dall'ISACA (*Information Systems Audit and Control Association*, Associazione per il controllo e l'audit dei sistemi informatici). COBIT aiuta le organizzazioni a conseguire obiettivi strategici tramite l'uso efficace delle risorse disponibili e la riduzione al minimo dei rischi informatici e mette in relazione la governance delle imprese alla governance informatica. Tale connessione avviene associando gli obiettivi delle imprese a quelli del settore informatico, definendo meccanismi di misurazione e modelli di maturità per misurare il conseguimento degli obiettivi e definire le responsabilità dei titolari delle imprese e dei processi informatici.

47 I temi affrontati negli audit sulla cibersicurezza sono estremamente vari. Alcune ISC hanno sottoposto ad audit settori di pubblico interesse assai specifici; l'audit svolto dall'ISC dei Paesi Bassi, ad esempio, ha esaminato la cibersicurezza delle sue difese costiere e dei suoi sistemi di gestione delle acque essenziali. Altre, come quella irlandese e quella ungherese, hanno affrontato questioni più orizzontali, come l'attuazione della strategia nazionale di cibersicurezza e la protezione dei dati personali e del patrimonio nazionale di dati. Comunque, tutte le ISC hanno analizzato questioni che potrebbero avere ripercussioni negative sulle infrastrutture o sui servizi pubblici.

48 Le ISC dell'Estonia e della Lituania hanno riconosciuto l'importanza strategica del patrimonio nazionale di dati, che è essenziale per la sicurezza nazionale, e della protezione della sua integrità dai ciberattacchi esterni. L'ISC danese ha dedicato un audit specifico alla valutazione della sicurezza di quattro organismi pubblici in relazione agli attacchi con ransomware. Le ISC di Paesi Bassi, Polonia e Portogallo hanno realizzato audit sull'efficacia dei diversi sistemi informatici utilizzati a sostegno dei controlli di frontiera (rispettivamente presso l'aeroporto di Schiphol, il comando centrale delle guardie di frontiera e il ministero degli Affari interni e dell'amministrazione in Polonia e ai confini del Portogallo), che hanno pertanto anche esaminato il tema della sicurezza all'interno dell'UE.

Periodo di audit

49 Le relazioni di audit selezionate, contenute nel presente compendio, sono state pubblicate tra il 2014 e il 2020. La maggior parte copriva un periodo di audit di due anni o più; mentre quattro ISC (Danimarca, Estonia, Francia e Portogallo) hanno limitato l'audit a un periodo di un anno.

Obiettivi dell'audit

50 Nel realizzare il proprio lavoro di audit, le varie ISC che hanno contribuito al presente compendio hanno trattato un variegato mosaico di rischi. In tali contributi sono stati analizzati i rischi di minacce ai diritti dei singoli cittadini dell'UE derivanti dall'uso improprio di dati personali, il rischio per le istituzioni di non riuscire a svolgere un servizio pubblico importante o di subire limitazioni delle proprie prestazioni, di gravi conseguenze per la sicurezza pubblica, il benessere e l'economia dello Stato membro nonché per la cibersicurezza all'interno dell'UE. Almeno quattro ISC (Estonia, Ungheria, Paesi Bassi e Portogallo), hanno trattato nelle proprie relazioni di audit di cui al presente compendio tre o più argomenti tra quelli menzionati.

51 La cibersicurezza rimane di competenza degli Stati membri. Con il progressivo ampliarsi della normativa dell'UE, che nel corso del tempo è diventata anche più specifica, la maggior parte delle istituzioni e degli organismi sottoposti ad audit dalle ISC aveva già contribuito al conseguimento degli obiettivi strategici di cibersicurezza dell'UE, seppur in misura variabile. In Irlanda, ad esempio, l'*Office of the Comptroller and Auditor General* ha sottoposto a audit l'attuazione della direttiva sulla sicurezza delle reti e dei sistemi informativi, intesa a migliorare la resilienza delle reti e dei

sistemi informativi principali, e ha formulato suggerimenti su come renderla più efficace. Analogamente, l'audit effettuato dall'Ufficio statale di audit ungherese ha riguardato la conformità alle vigenti direttive dell'UE.

52 Nel ***riquadro 14*** sono anche segnalati i casi in cui l'esito dell'audit ha contribuito a incrementare la ciber-resilienza dei soggetti controllati o a ridurre il numero di ciber-reati, o potrebbe contribuire a elaborare politiche di ciberdifesa e a rafforzare le competenze, migliorare lo sviluppo di tecnologie e a progredire nella collaborazione a livello internazionale; sono questi in particolare gli obiettivi principali della strategia dell'UE per la cibersicurezza. Nella maggior parte dei casi, le raccomandazioni formulate dalle ISC hanno riguardato più di due obiettivi strategici tra quelli che l'UE intende realizzare.

53 Inoltre, mediante il lavoro di audit svolto dalle ISC, sono state individuate lacune in materia di sicurezza o di attuazione che hanno spinto le istituzioni sottoposte a audit a profondere ulteriori sforzi. Ad esempio, nel corso dell'audit, quattro istituzioni controllate in Danimarca avevano già iniziato ad attuare vari controlli di sicurezza orientati al futuro onde accrescere sensibilmente il livello di protezione dagli attacchi con ransomware, sviluppare le capacità di difesa e incrementare la ciber-resilienza, riducendo in tal modo la propria esposizione alla cibercriminalità in futuro.

54 La Corte osserva altresì che le raccomandazioni di audit sono state indirizzate a vari livelli di gestione e responsabilità, quali l'amministrazione centrale, ministeri e agenzie a livello operativo, o titolari di sistemi informatici.

Riquadro 14

Riepilogo delle attività di audit realizzate dalle ISC ai fini dei contributi riportati nel compendio (parte 1)

Principale aspetto considerato		Danimarca	Estonia	Irlanda	Francia	Lettonia	Lituania	Ungheria	Paesi Bassi	Polonia	Portogallo	Finlandia	Svezia	UE (Corte dei conti europea)
Tipo di audit	Controllo di gestione	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Audit di conformità							✓		✓				
	Analisi													✓
Approccio dell'audit	Analisi delle politiche	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Analisi delle procedure	✓	✓		✓		✓	✓		✓	✓	✓		
	Analisi dei sistemi	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Valutazione della validità mediante test diretti								✓		✓			
Minacce affrontate	Impatto sui diritti individuali		✓		✓			✓			✓			✓
	Impatto su infrastrutture o servizi pubblici	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Impatto sulla sicurezza nazionale		✓	✓		✓	✓	✓	✓		✓			
	Impatto sulla sicurezza nell'Unione europea	✓							✓		✓			✓

Riepilogo delle attività di audit realizzate dalle ISC ai fini dei contributi riportati nel compendio (parte 2)

Principale aspetto considerato		Danimarca	Estonia	Irlanda	Francia	Lettonia	Lituania	Ungheria	Paesi Bassi	Polonia	Portogallo	Finlandia	Svezia	UE (Corte dei conti europea)
Obiettivi strategici di cibersicurezza dell'UE trattati	Incremento della ciber-resilienza	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Riduzione della cibercriminalità	✓					✓							✓
	Sviluppo di politiche e capacità di difesa	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Sviluppo di risorse tecnologiche				✓	✓			✓				✓	
	Miglioramento della cooperazione internazionale (politiche)			✓				✓						✓
Livello dei destinatari delle raccomandazioni	Amministrazione centrale	✓	✓				✓					✓	✓	✓
	Livello operativo (ministeri e agenzie)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Titolari di sistemi informatici	✓			✓			✓	✓	✓				

Principali osservazioni di audit

55 Le principali osservazioni di audit formulate dalle ISC sono sintetizzate nelle sezioni seguenti.

Controlli di gestione

56 La ***Rigsrevisionen*** **danese** ha valutato se una selezione di istituzioni governative fondamentali si fosse dotata di una protezione soddisfacente contro i ransomware. Le istituzioni governative sono spesso bersaglio di ciberattacchi e attualmente i ransomware rappresentano una delle maggiori minacce per la cibersicurezza. L'audit ha interessato l'autorità danese competente per i dati sanitari, il ministero degli Affari esteri, Banedanmark (le ferrovie danesi) e l'agenzia danese per la gestione delle emergenze. Queste quattro istituzioni sono state selezionate in quanto responsabili dell'erogazione di servizi essenziali in materia di salute, affari esteri, trasporti e preparazione alle emergenze, settori nei quali l'accesso ai dati può rivestire un'importanza cruciale. L'audit ha rilevato che le quattro istituzioni non disponevano di una protezione soddisfacente contro i ransomware. Dall'audit è emerso che tali istituzioni non avevano attuato vari controlli di sicurezza comuni per attenuare gli attacchi. L'audit ha concluso affermando l'importanza che le istituzioni valutino la possibilità di attuare controlli di sicurezza orientati al futuro per accrescere la propria resilienza agli attacchi con ransomware.

57 La ***Riigikontroll*** **estone** ha riconosciuto che per mantenere l'indipendenza dell'Estonia è necessario non solo garantire la difesa fisica del territorio, ma anche proteggere i beni digitali di importanza cruciale per lo Stato. I beni digitali che più necessitano di protezione sono quelli che riguardano i cittadini, il territorio e la legislazione. Occorre però mettere in sicurezza anche i dati concernenti le proprietà, i beni immobiliari e i diritti dei residenti in Estonia. La Corte dei conti estone ha considerato la possibilità di minacce informatiche nel caso di un aggravamento dei problemi di sicurezza. Tali scenari di rischio e un aumento degli incidenti legati alla sicurezza dell'informazione, come ciberattacchi e fughe di dati, potrebbero mettere a rischio dati e banche dati di estrema importanza per lo Stato. Di conseguenza, l'audit ha esaminato in che modo lo Stato determinasse quali dati e banche dati fossero cruciali per garantire la sicurezza nazionale. Ha concluso che, nonostante l'applicazione

del sistema di sicurezza di base "ISKE"[63] su tre livelli sia obbligatoria per gli enti statali, numerose banche dati di importanza critica presentano ancora gravi carenze in termini di sicurezza delle informazioni.

58 In Irlanda l'***Office of the Comptroller and Auditor General*** ha esaminato i progressi compiuti in termini di misure di cibersicurezza adottate dalla creazione del centro nazionale irlandese di cibersicurezza. Il centro, gestito dal ministero delle Comunicazioni, l'azione per il clima e l'ambiente, è stato istituito nel 2011. La sua azione è rivolta in primo luogo a garantire la sicurezza delle reti dell'amministrazione pubblica, ad assistere aziende e cittadini nella tutela dei propri sistemi e a mettere in sicurezza le infrastrutture critiche nazionali. Dall'audit è emerso che, benché il centro nazionale di cibersicurezza assolva una funzione cruciale, il livello di risorse di cui ha fruito nei primi quattro anni di attività è stato di gran lunga inferiore a quello originariamente previsto; inoltre, la direzione strategica generale del centro mancava di un piano strategico. Era inoltre necessario fare maggiore chiarezza riguardo ai rispettivi ruoli degli organismi responsabili delle indagini sui ciber-reati e sugli incidenti relativi alla sicurezza nazionale. Inoltre, le disposizioni della direttiva UE sulla sicurezza delle reti e dei sistemi informativi concernenti lo sviluppo di una strategia nazionale non erano ancora state attuate.

59 La ***Cour des comptes*** **francese** ha esaminato "*Parcoursup*", una nuova piattaforma digitale che funge da fonte di informazioni sui corsi universitari disponibili e sui requisiti di accesso; la piattaforma si propone di migliorare la corrispondenza tra le attitudini e i risultati scolastici degli studenti degli istituti secondari e i contenuti dei corsi dell'istruzione terziaria. L'audit ha rilevato che il governo era riuscito a centralizzare l'accesso a tutti gli studi post-secondari grazie alla piattaforma digitale, al fine di gestire l'espansione della varietà dell'istruzione superiore. Il sistema precedente, tuttavia, era stato affrettatamente rielaborato e trasformato nel nuovo "*Parcoursup*", senza alcuna modifica strutturale di rilievo. Pertanto, non era stato posto rimedio alle vulnerabilità del sistema informatico in termini di sicurezza, prestazioni e solidità. La piattaforma presenta ancora gravi rischi in termini di qualità e continuità dei servizi pubblici e di sicurezza dei dati personali.

[63] ISKE è uno standard di sicurezza delle informazioni elaborato per il settore pubblico estone; è obbligatorio per le organizzazioni dell'amministrazione centrale e locale che gestiscono banche date/registri.

60 La ***Valsts Kontrole*** **lettone** ha portato a termine un controllo di gestione sull'efficienza delle infrastrutture pubbliche delle tecnologie dell'informazione e della comunicazione (TIC). L'audit si proponeva di verificare se l'amministrazione pubblica avesse adottato un approccio unificato alla gestione efficiente delle infrastrutture TIC e se le istituzioni avessero valutato i benefici della centralizzazione. È emerso che la riluttanza delle autorità a gestire a livello centrale le infrastrutture TIC aveva portato a predisporre una serie di locali server, con un sensibile incremento dei costi di manutenzione. La maggior parte dei locali server era esposta a minacce alla sicurezza: i centri dati non erano protetti in maniera adeguata dall'accesso fisico né da rischi ambientali. Inoltre, non era stata prevista alcuna prassi per lo svolgimento di valutazioni periodiche da parte delle istituzioni, per verificare se fosse più economico eseguire la manutenzione dell'infrastruttura TIC internamente, cooperare con un'altra istituzione oppure esternalizzare tale compito. In esito all'audit, è stato raccomandato di introdurre un sistema di monitoraggio periodico che consentirebbe di valutare l'insieme della pubblica amministrazione come un sistema unico.

61 La ***Valstybės kontrolė*** **lituana** ha riconosciuto l'importanza di impiegare le risorse informative elettroniche critiche dello Stato, quali la gestione delle finanze pubbliche, l'amministrazione fiscale e la sanità. La perdita di informazioni critiche e l'indisponibilità dei corrispondenti sistemi informativi potrebbero avere gravi ripercussioni sulla sicurezza pubblica, il benessere e l'economia. L'audit si proponeva di valutare la gestione (controllo generale) e la maturità delle risorse informative statali critiche. Ha individuato problemi sistemici sia nella formulazione, sia nell'attuazione della politica in materia di risorse informative statali e nel relativo meccanismo di gestione. L'audit ha concluso che il modesto livello di maturità delle risorse informative statali critiche era indicativo di debolezze nella formulazione e nell'attuazione della politica in materia, che tale situazione rendeva tali risorse più vulnerabili e che per potenziarne la sicurezza occorreva migliorare il meccanismo di gestione.

62 Nel 2018 la ***Corte dei conti*** dei **Paesi Bassi** ha deciso di effettuare audit sulla cibersicurezza nei settori di importanza cruciale per la società. Sono stati controllati anzitutto la gestione delle acque e i controlli automatizzati alle frontiere: la prima è vitale per una nazione situata in gran parte al di sotto del livello del mare, i secondi sono essenziali data la posizione dell'aeroporto di Amsterdam Schiphol, hub internazionale e porta d'ingresso nel paese. Il ministro delle Infrastrutture e della gestione delle acque ha indicato come "elementi critici" del settore della gestione delle acque una serie di strutture idriche gestite dalla direzione generale dei lavori pubblici e della gestione delle acque (l'entità controllata). Molti sistemi informatici utilizzati per il

funzionamento delle strutture idriche critiche risalgono agli anni Ottanta e Novanta, quando generalmente non si teneva conto della cibersicurezza. Il ministro della Difesa e il ministro della Giustizia e della sicurezza condividono la responsabilità dei controlli di frontiera effettuati dalle guardie di frontiera olandesi all'aeroporto di Schiphol. Entrambi i ministeri dispongono di sistemi informatici a cui le guardie di frontiera si affidano. Tali sistemi sono essenziali per le operazioni aeroportuali e vengono impiegati per trattare dati altamente sensibili. Ciò li rende un ambìto bersaglio di ciberattacchi a fini di sabotaggio, spionaggio o manipolazione dei controlli di frontiera. L'audit ha verificato se le entità controllate fossero preparate a gestire le minacce informatiche e se ciò avvenisse in modo efficace. Per quanto riguarda le strutture idriche, era necessario che l'entità controllata intensificasse gli sforzi in materia di individuazione e risposta, onde conseguire gli obiettivi di cibersicurezza perseguiti. Per quanto riguarda i controlli alla frontiera, si è constatato che le misure di cibersicurezza non erano né appropriate né adeguate alle esigenze future.

63 Il ***Tribunal de Contas*** **portoghese** ha sottoposto ad audit i sistemi informativi su cui si basano la concessione, il rilascio e l'utilizzo del passaporto elettronico portoghese (PEP), soprattutto per quanto riguarda lo screening automatizzato dei passeggeri tramite lettura dei dati biometrici alle frontiere del Portogallo. L'audit ha verificato la conformità alla normativa nazionale e dell'UE, alle norme internazionali e agli orientamenti per la concessione, il rilascio e l'utilizzo del PEP, compresa l'adeguatezza del quadro giuridico nazionale. È stata esaminata l'efficacia dei principali processi associati al ciclo di vita del PEP, in particolare per quanto riguarda la concessione, il rilascio e l'utilizzo. Inoltre, l'audit ha analizzato aspetti cruciali della performance dei sistemi informativi, in particolare il rispetto dei requisiti di sicurezza dei sistemi informativi del PEP (SIPEP).

64 La ***Valtiontalouden tarkastusvirasto*** **finlandese** ha verificato se la ciberprotezione nell'amministrazione centrale fosse il più possibile efficace ed efficiente in termini di costi. L'audit era incentrato sulla gestione della cibersicurezza da parte dell'amministrazione centrale. Le entità sottoposte ad audit comprendevano le autorità preposte alla ciberprotezione nell'amministrazione centrale (l'ufficio del primo ministro, il ministero delle Finanze e il ministero dei Trasporti e delle comunicazioni), nonché le autorità responsabili delle funzioni di ciberprotezione centralizzata e dei servizi informatici centralizzati nell'amministrazione centrale. Nel governo finlandese la responsabilità della ciberprotezione è decentrata: ogni organismo interno è responsabile della propria cibersicurezza. Si è raccomandato al ministero delle Finanze di definire e attuare un modello complessivo di gestione

operativa nel caso di incidenti di cibersicurezza che interessino i servizi TIC dell'amministrazione centrale. Il ministero delle Finanze dovrebbe anche individuare le modalità per affrontare la questione della cibersicurezza dei servizi nei servizi di finanziamento durante il loro intero ciclo di vita; dovrebbe inoltre accrescere la consapevolezza situazionale a livello operativo, prescrivendo alle autorità di segnalare le violazioni informatiche al centro di cibersicurezza.

65 La ***Riksrevisionen*** **svedese** si è occupata dell'incidenza dei sistemi informatici obsoleti nell'amministrazione centrale, onde valutare se il governo e le autorità avessero adottato misure adeguate per impedire che i sistemi informatici diventassero un ostacolo a un'efficace digitalizzazione. L'audit ha individuato sistemi informatici obsoleti in un gran numero di agenzie pubbliche. Presso molte agenzie sottoposte a audit, uno o più sistemi informatici critici per l'attività erano obsoleti; una cospicua percentuale delle agenzie esaminate non adottava un approccio corretto allo sviluppo e all'amministrazione del sostegno informatico. Larga parte delle agenzie era priva di una descrizione globale dei collegamenti tra strategie, sistemi e processi operativi. Si è concluso che gran parte delle agenzie non era ancora riuscita a gestire efficacemente i problemi derivanti dall'obsolescenza dei sistemi informatici. L'istituzione superiore di controllo svedese giudica il problema così grave e diffuso da ostacolare una continua ed efficiente digitalizzazione dell'amministrazione statale.

Audit di conformità dedicati alla cibersicurezza

66 L'***Ufficio statale di audit*** **ungherese** ha riconosciuto che la sicurezza del patrimonio nazionale di dati rappresenta un fondamentale interesse della società per la conservazione e la protezione dei valori nazionali. Il potenziamento della sicurezza dei dati personali e pubblici nell'ambito del patrimonio nazionale di dati dell'Ungheria è essenziale per consolidare la fiducia dei cittadini nello Stato e assicurare il costante e corretto funzionamento dell'amministrazione pubblica. L'audit di conformità sulla protezione dei dati si prefiggeva l'obiettivo di valutare se in Ungheria fosse stato istituito un quadro normativo e operativo per la protezione dei dati e se le più importanti organizzazioni di gestione dei dati avessero rispettato le disposizioni in materia di gestione sicura dei dati ed esternalizzazione del loro trattamento. L'audit ha concluso che le norme interne delle organizzazioni di gestione dei dati in materia di attività di gestione dei dati garantivano la protezione del patrimonio nazionale di dati nell'ambito del patrimonio nazionale, conformemente alle disposizioni giuridiche in vigore fra il 2011 e il 2015. I titolari del trattamento dei dati avevano attuato

correttamente le disposizioni e il trasferimento dei dati a terzi si era svolto in maniera adeguata.

67 La ***Najwyższa Izba Kontroli*** **polacca** ha valutato se i dati raccolti nei sistemi destinati ad assolvere importanti funzioni pubbliche fossero sicuri. L'audit ha interessato sei istituzioni selezionate responsabili di importanti funzioni pubbliche. Il grado di preparazione e attuazione del sistema di sicurezza delle informazioni non ha garantito un livello di sicurezza accettabile per i dati raccolti nei sistemi informatici utilizzati per svolgere importanti funzioni pubbliche. I processi di sicurezza delle informazioni si svolgevano in maniera disordinata e, in mancanza di procedure, intuitiva. Tra le sei unità sottoposte ad audit, soltanto una aveva attuato il sistema di sicurezza delle informazioni; va tuttavia osservato che il suo funzionamento aveva presentato comunque gravi difetti. L'audit ha concluso che le raccomandazioni generali e le disposizioni in materia di sicurezza informatica devono essere sviluppate e attuate a livello centrale; tale considerazione vale per tutti gli enti pubblici.

Analisi della cibersicurezza

68 La ***Corte dei conti europea*** ha esaminato il quadro della politica dell'UE in materia di cibersicurezza, individuando le principali sfide a un'efficace attuazione di tale politica. L'audit ha riguardato i temi della sicurezza delle reti e dell'informazione, della cibercriminalità, della ciberdifesa e della disinformazione. Sono state rilevate una serie di carenze nella normativa UE in materia di cibersicurezza e si è rilevato che la legislazione vigente non è stata recepita in maniera coerente dagli Stati membri. Infine, l'analisi ha richiamato l'attenzione sulla carenza di dati attendibili sui ciberincidenti a livello di UE e sulla mancanza di un quadro complessivo delle spese in materia di cibersicurezza sostenute dall'UE e dagli Stati membri. L'analisi ha inoltre rilevato la scarsa adeguatezza delle risorse assegnate alle agenzie dell'UE operanti nei settori in cui la cibersicurezza è importante e che, fra l'altro, dette agenzie hanno difficoltà ad attrarre e trattenere persone di talento. Un'altra sfida riguarda il disallineamento tra i finanziamenti a favore della cibersicurezza e gli obiettivi strategici dell'UE.

PARTE III – Sintesi delle relazioni delle ISC

Danimarca
Rigsrevisionen

Protezione contro gli attacchi con ransomware

Data di pubblicazione: 2017

Link alla relazione: Sintesi della relazione (versione inglese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: Aprile – settembre 2017

Sintesi della relazione

Tema dell'audit

Questa relazione ha verificato se una selezione di istituzioni governative essenziali si fosse dotata di una protezione soddisfacente contro i ransomware.

Le istituzioni governative sono spesso bersaglio di ciberattacchi e attualmente i ransomware rappresentano una delle maggiori minacce per la cibersicurezza. Un ransomware è un software malevolo che blocca l'accesso ai dati. In generale il ransomware crittografa i dati e impedisce alle istituzioni attaccate di utilizzarli. Gli hacker chiedono un riscatto per decifrare i dati e consentire alle istituzioni di accedervi nuovamente. Di conseguenza i ransomware rappresentano una minaccia particolare per l'accessibilità dei dati.

L'improvvisa impossibilità di accedere ai dati può ostacolare le istituzioni nell'erogazione di importanti servizi, o può impedire del tutto la prestazione di tali servizi. Le istituzioni colpite da un attacco con ransomware sono generalmente costrette a chiudere la propria rete informatica in tutto o in parte per indagare la portata dell'attacco. Gli attacchi con ransomware possono avere un grave impatto economico poiché le istituzioni rischiano di subire una perdita di produzione, se per esempio non possono accedere alla propria rete informatica oppure sono andati

perduti i dati raccolti e trattati in un arco di tempo ampio. Nel 2017, un attacco con ransomware al servizio sanitario nazionale britannico ha provocato la cancellazione di 19 000 operazioni e appuntamenti. La dirigenza delle istituzioni dovrebbe pertanto concentrare l'attenzione sul rischio di attacchi con ransomware e attuare i necessari controlli di sicurezza per proteggersi contro i ransomware e ridurre l'impatto di un potenziale attacco.

Lo studio ha interessato l'autorità danese competente per i dati sanitari, il ministero degli Affari esteri, Banedanmark (le ferrovie danesi) e l'agenzia danese per la gestione delle emergenze. Queste quattro istituzioni sono state selezionate in quanto responsabili dell'erogazione di servizi essenziali in materia di salute, affari esteri, trasporti e preparazione alle emergenze, settori nei quali l'accesso ai dati può rivestire un'importanza cruciale. L'autorità competente per i dati sanitari fornisce anche servizi informatici centralizzati a gran parte degli organismi governativi che dipendono dal ministero della Salute.

Lo studio si proponeva di valutare se le quattro istituzioni si fossero dotate di una protezione soddisfacente contro gli attacchi con ransomware perpetrati via e-mail. La *Rigsrevisionen* ha pertanto esaminato 20 controlli di sicurezza comuni che forniscono una protezione di base contro i ransomware. L'ISC ha inoltre esaminato cinque controlli di sicurezza che le istituzioni dovrebbero prendere in considerazione riguardo alle future valutazioni dei rischi. Tra i controlli orientati al futuro rientra, per esempio, una nuova tecnologia che può ridurre il numero di e-mail false che accedono a un'istituzione oppure può individuare le attività insolite su computer e inviare segnali di allarme. Lo studio è stato avviato dalla *Rigsrevisionen* e si basa sulle constatazioni di quattro audit in materia di tecnologie dell'informazione effettuati tra aprile e settembre 2017; esso offre un'istantanea del livello di protezione delle istituzioni nei confronti dei ransomware. Le istituzioni hanno avuto l'opportunità di attuare i 20 controlli di sicurezza comuni dopo il completamento degli audit in materia di tecnologie dell'informazione. Pertanto, i risultati dello studio riguardano solo la protezione delle istituzioni dai ransomware nel periodo in cui sono stati effettuati i quattro audit. Lo studio offre un'immagine della performance delle quattro istituzioni, ma non contiene un'analisi comparativa né una graduatoria delle performance.

Constatazioni e conclusioni

Secondo la valutazione della *Rigsrevisionen*, le quattro istituzioni non disponevano di una protezione soddisfacente contro i ransomware. Dallo studio è emerso che le quattro istituzioni non avevano attuato vari controlli di sicurezza comuni per attenuare gli attacchi. In particolare l'autorità competente per i dati sanitari e Banedanmark dimostravano considerevoli lacune in materia di sicurezza. Ciò implica che tutte e quattro le istituzioni fossero esposte a un crescente rischio di attacchi con ransomware perpetrati via e-mail che avrebbero impedito loro di prestare i propri servizi per periodi di tempo variabili. Dopo il completamento dello studio, tutte e quattro le istituzioni hanno informato la *Rigsrevisionen* di aver provveduto ad attuare numerosi controlli di sicurezza, allo scopo di migliorare il livello di protezione contro i ransomware.

La prevenzione degli attacchi con ransomware prevista da queste istituzioni, comprese le minacce sia interne che esterne, era inadeguata. Desta particolare preoccupazione il fatto che nessuna delle istituzioni assicurasse l'aggiornamento delle patch dei software di sicurezza e che tre delle istituzioni non avessero creato "liste bianche" per scongiurare la possibilità che il personale introducesse malware. Ciò aggrava il rischio che il ransomware infetti in tutto o in parte la rete informatica e si diffonda.

In tre delle istituzioni, la dirigenza non era sufficientemente consapevole della minaccia rappresentata dai ransomware e le valutazioni dei rischi effettuate dalla dirigenza dell'autorità competente per i dati sanitari e di Banedanmark non coprivano tutti gli aspetti pertinenti. Di conseguenza, le istituzioni non disponevano di una valutazione aggiornata della minaccia rappresentata dai ransomware e si trovavano pertanto in una posizione debole nella prevenzione di nuovi attacchi e nella riduzione dell'impatto di attacchi futuri. I dirigenti dell'autorità competente per i dati sanitari e di Banedanmark non hanno concentrato sufficiente attenzione sulla valutazione del rischio; la sicurezza informatica in queste due istituzioni, pertanto, non era basata sulle priorità definite dalla dirigenza stessa.

Tre delle istituzioni non avevano predisposto adeguati piani di risposta agli incidenti, tali da consentire il ripristino delle operazioni dopo un attacco con ransomware. È particolarmente significativo che tre di queste istituzioni non verificassero periodicamente la propria capacità di ripristinare dati e sistemi colpiti da un attacco con ransomware. Ciò aumenta il rischio che i dati detenuti da queste istituzioni vadano perduti in conseguenza di un attacco con ransomware e che le istituzioni stesse non riescano a prestare i propri servizi per un periodo di tempo prolungato.

Dal momento che gli scenari di rischio sono in costante evoluzione, è importante che le istituzioni prendano in considerazione la possibilità di attuare controlli di sicurezza orientati al futuro per migliorare la propria resilienza ad attacchi con ransomware, ossia controlli che rendano più facile verificare l'identità dei mittenti delle e-mail e siano in grado di individuare e filtrare le e-mail potenzialmente nocive. Tutte e quattro le istituzioni stanno attualmente lavorando ad alcuni dei controlli di sicurezza orientati al futuro che possono contribuire a migliorare la protezione contro gli attacchi con ransomware.

Altre relazioni in questo settore

Titolo della relazione:	Relazione sulla protezione dei dati di ricerca presso le università danesi
Link alla relazione:	Sintesi della relazione (versione inglese)
Data di pubblicazione:	2019
Titolo della relazione:	Relazione sulla protezione dei sistemi informatici e dei dati sanitari in tre regioni della Danimarca
Link alla relazione:	Sintesi della relazione (versione inglese)
Data di pubblicazione:	2017
Titolo della relazione:	Relazione sulla gestione della sicurezza informatica nei sistemi esternalizzati a fornitori esterni
Link alla relazione:	Sintesi della relazione (versione inglese)
Data di pubblicazione:	2016
Titolo della relazione:	Relazione sull'accesso ai sistemi informatici su cui si fonda l'erogazione di servizi essenziali alla società danese
Link alla relazione:	Sintesi della relazione (versione inglese)
Data di pubblicazione:	2015

Estonia
Riigikontroll

Garantire la sicurezza e la preservazione delle banche dati statali di importanza critica in Estonia

Data di pubblicazione: Maggio 2018

Link alla relazione: Sintesi della relazione (versione inglese)
Relazione (versione estone)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2017

Sintesi della relazione

Tema dell'audit

Per mantenere l'indipendenza dell'Estonia è necessario non solo difenderne fisicamente il territorio, ma anche proteggere i beni digitali di importanza cruciale per lo Stato dagli eventi che rappresentano la minaccia più grave. I beni digitali che più necessitano di protezione sono quelli che riguardano i cittadini, il territorio e la legislazione. Occorre però mettere in sicurezza anche i dati concernenti le proprietà, i beni immobiliari e i diritti dei residenti in Estonia.

L'istituzione superiore di controllo nazionale ha esaminato in che modo lo Stato avesse stabilito quali dati e banche dati fossero cruciali per garantire la sicurezza nazionale. È stata controllata la protezione della sicurezza e della continuità di questi dati e banche dati, anche mediante una panoramica degli strumenti usati per la protezione.

Dal momento che oggi l'Estonia fa parte della NATO e dell'Unione europea, la sicurezza fisica del paese è garantita in maniera più efficace rispetto al periodo precedente all'adesione a queste due organizzazioni. L'Estonia deve però considerare la possibilità di minacce informatiche nel caso di un aggravamento dei problemi di sicurezza. Tali scenari di rischio e un aumento degli incidenti legati alla sicurezza dell'informazione,

come ciberattacchi e fughe di dati, potrebbero anche mettere a rischio dati e banche dati di estrema importanza per lo Stato. Se dati di primaria importanza per lo Stato dovessero essere modificati senza autorizzazione, trapelassero o andassero perduti, lo Stato non sarebbe più in grado di assolvere le funzioni necessarie, quali garantire la sicurezza dei cittadini, provvedere alle loro necessità, creare il contesto necessario all'attività economica e molto altro. L'Estonia prevede inizialmente di spendere circa un milione di euro per archiviare all'estero dati critici.

Quesiti di audit

- I ministeri hanno individuato tutte le banche dati critiche e i requisiti relativi al trattamento?
- Banche dati e registri critici sono stati messi in sicurezza?
- È garantita la continuità di banche dati e dati critici nel lungo periodo?

Constatazioni

L'istituzione superiore di controllo nazionale ha formulato le seguenti osservazioni in merito alle banche dati critiche sottoposte a audit:

- non erano stati predisposti piani d'azione né requisiti intesi ad attuare concretamente il concetto di banche dati critiche. Le condizioni di selezione delle banche dati critiche non erano state determinate e non vi era certezza che tutte le banche dati necessarie fossero incluse nel processo. La protezione supplementare delle banche dati era stata organizzata in maniera informale e non era obbligatoria per i titolari delle banche dati: per questo motivo non è stato effettuato un back-up all'estero dei dati delle cinque banche dati critiche;
- per le banche dati critiche non erano state stabilite norme supplementari di sicurezza delle informazioni. Né il sistema di sicurezza delle informazioni ISKE (uno standard di sicurezza delle informazioni elaborato per il settore pubblico estone, obbligatorio per le organizzazioni dell'amministrazione centrale e locale che gestiscono banche dati/registri), né altre norme o atti giuridici contenevano requisiti supplementari relativi alle banche dati critiche, quali il back-up dei dati al di fuori dell'Estonia. Le copie di back-up delle banche dati sottoposte a audit venivano trasferite all'estero, ma il recupero del lavoro dei sistemi di informazione da tali banche dati non era stato testato;

- l'attuazione di ISKE e il relativo lavoro di audit hanno rappresentato un problema in relazione alle banche dati critiche. Al momento dell'audit non erano stati effettuati audit ISKE su due delle 10 banche dati, e gli audit erano stati organizzati soltanto alla fine di quest'audit (30 novembre 2017). Solo due banche dati critiche erano state sottoposte a audit con la frequenza richiesta dalla legge. Si sono verificati casi in cui i problemi evidenziati dagli auditor non erano stati risolti nel periodo intercorso tra i due audit ISKE (due-tre anni).

- Durante l'audit, l'istituzione superiore di controllo nazionale ha rilevato che in alcune banche dati critiche non erano state attuate importanti misure di sicurezza delle informazioni. Ad esempio, i requisiti per la valutazione periodica delle vulnerabilità dei sistemi informativi non erano stati definiti in orientamenti sulla sicurezza delle informazioni; non erano stati effettuati controlli regolari né analisi dei registri eventi; non esistevano piani di formazione in materia di sicurezza delle informazioni né analisi delle conoscenze in materia di sicurezza delle informazioni in quei settori della pubblica amministrazione che costituiscono la base di tali piani di formazione; in alcuni casi non era stata verificata l'integrità dei file e non erano stati effettuati test di penetrazione esterni.

Conclusioni e raccomandazioni

Dall'audit è emerso che, nonostante l'attuazione del sistema di sicurezza di base su tre livelli ISKE, il cui uso è obbligatorio per gli enti statali e i relativi audit, permanevano gravi carenze in termini di sicurezza delle informazioni in numerose banche dati critiche riguardo, ad esempio, all'analisi dei registri, ai test di penetrazione e alla protezione dei dispositivi mobili. Non erano ancora stati definiti i requisiti specifici necessari alla protezione dei dati critici.

Il ministero degli Affari economici e delle comunicazioni aveva avviato le prime attività necessarie alla protezione di dati critici, ma il progetto relativo alle banche dati critiche si trovava in una fase in cui avrebbe richiesto un insieme di norme giuridicamente vincolante. Non esistevano neppure un'analisi dei rischi dettagliata, né un piano d'azione per il futuro.

Copie di back-up di cinque banche dati critiche erano conservate presso ambasciate in paesi stranieri, ma in caso di distruzione fisica dei centri dati ubicati in Estonia, la preservazione dei dati critici nelle cinque banche dati rimanenti non sarebbe stata garantita.

Sono state formulate due raccomandazioni di carattere generale:

- determinare le norme per la protezione supplementare delle banche dati critiche, tra cui la selezione delle banche dati critiche, il trattamento dei dati in queste banche dati e il back-up dei dati di importanza critica per lo Stato; nonché valutare come stanziare finanziamenti supplementari per tali attività;
- analizzare le diverse fasi di costituzione delle banche dati, in termini di pianificazione finanziaria e di sicurezza delle informazioni, e attuare le migliori prassi di gestione dei progetti nello svolgimento di tali fasi.

Irlanda
Office of the Comptroller and Auditor General

Misure concernenti la cibersicurezza nazionale

Data di pubblicazione: Settembre 2018

Link alla relazione: Sintesi della relazione (versione inglese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2011-2018

Sintesi della relazione

Tema dell'audit

In Irlanda, il ministero delle Comunicazioni, l'azione per il clima e l'ambiente è responsabile della politica in materia di cibersicurezza. Tramite il centro nazionale di cibersicurezza, il ministero è responsabile altresì del coordinamento della risposta pubblica alle emergenze per qualunque incidente di cibersicurezza a livello nazionale.

Il centro nazionale di cibersicurezza è stato istituito nel 2011. La sua azione è rivolta in primo luogo a garantire la sicurezza delle reti dell'amministrazione pubblica, ad assistere aziende e cittadini nella tutela dei propri sistemi e a mettere in sicurezza le infrastrutture critiche nazionali.

Quesiti di audit

L'audit esamina i progressi compiuti in termini di misure di cibersicurezza dopo l'istituzione del centro nazionale di cibersicurezza. In particolare analizza le questioni concernenti:

- il mandato e l'assegnazione di risorse per il centro;

- la strategia nazionale di cibersicurezza (2015-2017);
- l'attuazione della direttiva UE sulla sicurezza delle reti e dei sistemi informativi;
- disposizioni di governance e di supervisione.

Constatazioni e conclusioni

La decisione del governo sull'istituzione del centro nazionale di cibersicurezza ha approvato un finanziamento annuale di 800 000 euro; tuttavia, tra il 2012 e il 2015 il finanziamento annuale effettivo a favore della cibersicurezza è stato inferiore a un terzo di tale importo. Nel 2017 la dotazione è aumentata a 1,95 milioni di euro. Nel corso del 2017 il personale del centro è quasi raddoppiato, raggiungendo 14,5 equivalenti a tempo pieno. Nel 2018 è stata approvata la nomina di altri 16 addetti.

La strategia nazionale di cibersicurezza (2015-2017) ha definito 12 misure da realizzare nel tempo di vita della strategia. A maggio del 2018 erano state portate a termine quattro misure, quattro erano state attuate parzialmente, e quattro non erano state attuate affatto.

La direttiva UE sulla sicurezza delle reti e dei sistemi informativi si propone di migliorare la resilienza delle reti e dei sistemi informativi principali. In Irlanda, da una valutazione dei progressi relativi a ciascuno dei tre pilastri contenuti nella direttiva, è emerso quanto segue:

- *pilastro 1 – migliorare le capacità di cibersicurezza degli Stati membri dell'UE:* parzialmente attuato. Si è ottemperato ai requisiti strutturali, ma rimangono carenze nella pianificazione strategica;
- *pilastro 2 – agevolare la cooperazione in materia di cibersicurezza tra gli Stati membri dell'UE:* attuato;
- *pilastro 3 – introdurre misure di sicurezza e obblighi di segnalazione degli incidenti per i settori essenziali:* parzialmente attuato. C'è ancora strada da fare in merito all'individuazione delle reti e dei sistemi informativi critici, all'indicazione formale delle entità che saranno designate come operatori di servizi essenziali e alla gestione dei fornitori di servizi digitali.

La decisione con cui, nel luglio 2011, il governo ha approvato l'istituzione del centro nazionale di cibersicurezza ha sancito altresì la formazione di una commissione interministeriale incaricata di definire e attuare la strategia per rispondere alle sfide poste dalla cibersicurezza in Irlanda. Il gruppo si è riunito cinque volte dal 2013 al 2015, ma è stato possibile esaminare i verbali di una sola riunione. La commissione non si riunisce dal 2015.

Il piano di attuazione della strategia nazionale di cibersicurezza prevedeva l'impegno a pubblicare una relazione annuale e a svolgere una valutazione d'impatto formale del lavoro a fine 2017. Questi impegni non sono ancora stati onorati, benché l'operato del centro sia descritto nella relazione annuale del ministero.

Quest'ultimo ha richiesto formalmente una valutazione della performance del centro. Non è stato fornito alcun elemento attestante lo svolgimento di una tale valutazione. Il ministero ha affermato che la valutazione della performance del centro nazionale di cibersicurezza faceva parte della normale gestione della performance e della governance interna del ministero.

In esito all'audit, sono state tratte le seguenti conclusioni:

- benché il centro nazionale di cibersicurezza assolva una funzione critica, il livello di assegnazione di risorse per i primi quattro anni di attività è stato sensibilmente inferiore a quello originariamente previsto;
- la direzione strategica complessiva del centro non è chiara e attualmente non esiste un piano strategico;
- occorre maggiore chiarezza per quanto riguarda i rispettivi ruoli degli organismi coinvolti nelle indagini sui reati informatici e sugli incidenti che interessano la sicurezza nazionale;
- si attende ancora l'attuazione delle disposizioni della direttiva UE sulla sicurezza delle reti e dei sistemi informativi concernenti l'elaborazione di una strategia nazionale;
- sono state previste strutture di governance, ma non è chiaro come i relativi meccanismi operino di fatto.

Vi è scarsa trasparenza per quanto riguarda la disponibilità e il costo delle risorse dedicate alla cibersicurezza.

Francia
Cour des comptes

Accesso all'istruzione superiore: una valutazione iniziale della legge sull'orientamento e il successo degli studenti

Data di pubblicazione: Febbraio 2020

Link alla relazione: Relazione (versione francese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2019-2020

Sintesi della relazione

Tema dell'audit

La legge del 2018 sull'orientamento e il successo degli studenti (*loi relative à l'orientation et à la réussite des étudiants*, ORE) si proponeva di migliorare le tre fasi principali del percorso seguito dai giovani che accedono all'istruzione superiore: orientamento e sostegno per gli studenti delle scuole secondarie superiori, selezione dei corsi e buon esito dei primi anni di studio. La legge ha introdotto "*Parcoursup*", una nuova piattaforma digitale che funge da fonte di informazioni sui corsi universitari disponibili e sui requisiti di accesso, il cui scopo è migliorare la corrispondenza tra le attitudini e i risultati degli studenti degli istituti secondari e i contenuti dei corsi dell'istruzione terziaria.

Nei primi due anni dall'emanazione dell'ORE è stato compiuto il primo passo verso la trasformazione dell'accesso all'istruzione superiore. Nonostante vari vincoli, l'introduzione di "*Parcoursup*" è avvenuta senza alcuna difficoltà, benché mancassero ancora garanzie di sicurezza e sostenibilità, e benché i dati potessero essere sfruttati meglio, data la loro importanza.

L'ORE è stata introdotta per risolvere due gravi problemi della politica dell'istruzione: il primo era l'elevato tasso di abbandono tra gli studenti universitari e il secondo era la profonda insoddisfazione per la precedente piattaforma digitale che, nella fase finale, utilizzava una selezione casuale.

Per la riforma dell'ORE sono stati erogati finanziamenti pari a 867 milioni di euro nell'arco di cinque anni. Essa si basava sul concetto di un continuum "-3/+3" e sul principio di fondo per cui quanto più gli studenti degli istituti secondari superiori erano a conoscenza dei contenuti dei corsi dell'istruzione terziaria, tanto maggiori erano le loro possibilità di superare gli esami, poiché avrebbero scelto i corsi che più corrispondevano alle proprie attitudini e ambizioni. L'ORE cercava di sopperire alla mancanza di orientamento per gli studenti degli istituti secondari superiori, riducendo così i trasferimenti di corso, che secondo le stime della *Cour* avevano un costo di quasi 550 milioni di euro all'anno per il solo primo anno di istruzione superiore.

Gli auditor hanno svolto una valutazione iniziale dell'accesso all'istruzione superiore nel contesto dell'ORE, esaminando le questioni relative alla sicurezza informatica sollevate dalla piattaforma.

Il sistema informativo era caratterizzato da un'espansione dei fattori di carico (l'inclusione nel 2020 di tutti i corsi di istruzione superiore e il rapido incremento del numero di utenti nel giro di pochi anni). La causa è da ricercarsi nel rapido passaggio dalla precedente piattaforma "*Parcoursup*" senza modificarne l'architettura, che ha così generato notevoli rischi in termini di qualità, continuità, adattabilità e ulteriore sviluppo del servizio. Le debolezze del sistema in materia di sicurezza, performance e solidità non erano state corrette. È stato possibile allestire rapidamente "*Parcoursup*" perché esso era gestito in modalità beta da un piccolo gruppo di persone altamente qualificate e motivate, ma a causa di tale approccio sono venute a mancare una direzione strategica e una governance soddisfacente.

Gli auditor hanno valutato la qualità del sistema informativo e la performance della nuova piattaforma "*Parcoursup*". "*Parcoursup*" è stata istituita nell'ambito dell'ORE per migliorare la qualità dell'assegnazione ai corsi di istruzione superiore e, in tal modo, aumentare il tasso di conseguimento del diploma di laurea.

Constatazioni

Pur funzionando in maniera soddisfacente, la piattaforma "*Parcoursup*" era esposta a rischi informatici che occorreva ridurre. Erano necessarie garanzie sulla sicurezza e la sostenibilità della piattaforma e si sarebbe potuto fare un miglior uso dei dati.

Un sistema informativo obsoleto

"*Parcoursup*" aveva pochi elementi di novità e aveva ereditato la farraginosa complessità e la fragilità della precedente piattaforma "*Admission post-bac*" (APB), assieme a molti rischi non risolti. Il sistema informativo che costituiva la base strutturale di "*Parcoursup*" era stato ripreso direttamente dalla piattaforma precedente. Benché fosse stato presentato come un nuovo strumento di assegnazione, il nucleo del sistema informativo era stato modificato solo lievemente rispetto all'APB. In realtà, oltre il 72 % dell'infrastruttura informatica era restato immutato, in quanto poco meno del 30 % del codice APB era stato riscritto.

Le basi informatiche della piattaforma erano state concepite all'inizio degli anni 2000 allo scopo di gestire approssimativamente un milione di domande per circa 100 000 posti ogni anno; in seguito, tuttavia, la portata del sistema informativo è stata ampliata per gestire un afflusso annuale di 10 milioni di domande per un milione di posti circa. "*Parcoursup*" si è rivelato un vecchio strumento con una denominazione nuova. L'incremento di carico sollevava dubbi sulla capacità della piattaforma di raggiungere lo scopo perseguito.

Un sistema informativo inadeguatamente documentato

Nonostante gli sforzi di trasparenza compiuti dal ministero, il codice sorgente di "*Parcoursup*" era ancora chiuso al 99 %. Il poco che era stato pubblicato era di scarso interesse ai fini della comprensione, della verifica e della valutazione del processo che assegnava i candidati ai corsi.

Come la piattaforma che l'aveva preceduta, "*Parcoursup*" era un sistema informativo operativo inadeguatamente documentato. I risultati dell'audit condotto sul codice indicano che l'applicazione era di cattiva qualità e ad alto rischio; l'audit ha individuato numerose violazioni critiche. Il sistema era di qualità inferiore a quella di altri software dello stesso periodo e presentava forti rischi di crash.

"*Parcoursup*" utilizzava codici sorgente pubblici e chiusi. Il codice pubblico presentava un tasso di violazioni critiche assai più elevato del codice chiuso, il che implicava un rischio di interruzioni del servizio; la piattaforma non era neppure a prova di hacker (audit del luglio 2018 sulla sicurezza del codice sorgente). Alla fine del 2019, il ministero ha però annunciato che era iniziata una procedura di certificazione per il codice "*Parcoursup*".

La documentazione esistente per il codice sorgente non era né coerente né esaustiva. Il codice "*Parcoursup*" era contraddistinto da un'anomala complessità. A giudizio degli auditor, il codice sorgente dovrebbe essere ristrutturato per ridurre il numero di componenti complesse.

L'architettura del sistema informativo di "*Parcoursup*" era ad alto rischio; aspetto davvero arcaico, la banca dati veniva gestita manualmente. Il sistema era fragile a causa della forte dipendenza dalla disponibilità e dalla vigilanza dell'operatore. Il ministero ha riconosciuto che questi alti rischi erano connessi all'architettura di "*Parcoursup*" e che quindi non era possibile correggerli senza sviluppare ulteriormente l'applicazione.

Il sistema informativo di "*Parcoursup*" era inadeguatamente documentato e dipendeva essenzialmente dalle competenze del personale dell'agenzia governativa nazionale (*Service à compétence nationale*, SCN). A fini di documentazione, una serie di osservazioni era stata scritta nella banca dati al centro del sistema, rendendo difficili la manutenzione e lo sviluppo del sistema informativo e l'utilizzo dei dati. Non era semplice estrarre né valutare le informazioni degli utenti presenti sulla piattaforma senza un'indagine approfondita. Data l'assenza di una documentazione tecnica strutturata, la capacità dell'SCN di assolvere le proprie funzioni strategiche dipendeva interamente dal responsabile del centro informatico.

Strategia di sicurezza: sono necessari miglioramenti

Considerata la sensibilità dei dati personali contenuti nel sistema, "*Parcoursup*" rappresenta una vera sfida in termini di sicurezza. In linea di principio, tutte le organizzazioni che gestiscono un sistema informativo devono dotarsi di una politica sulla sicurezza dei sistemi informativi (*information systems security policy*, ISSP) formale e scritta. Benché riconosciuto dal primo ministro come un fornitore di servizi essenziali, "*Parcoursup*" non disponeva di una ISSP. Era necessario un intervento immediato per predisporne una.

Ciascuna équipe di "*Parcoursup*" aveva un responsabile della sicurezza dei sistemi informativi (*information systems security officer*, ISSO) distaccato presso il centro informatico. Sarebbe stato opportuno distaccare gli ISSO direttamente presso il direttore dell'SCN per garantirne l'indipendenza.

A metà del 2019, era ancora in corso il processo per rendere "*Parcoursup*" conforme al GDPR. Alcune misure erano ancora in sospeso, tra cui in particolare la necessità di stabilire formalmente le varie procedure utilizzate per il trattamento. La sicurezza dei dati personali rimaneva inadeguata e si conservava ancora una quantità troppo elevata di dati individuali completi.

L'unità "*Parcoursup*" faceva capo sia al responsabile del progetto "*Parcoursup*", nominato dall'ufficio del ministro, sia al dipartimento per gli affari studenteschi e la strategia di formazione della direzione generale per l'istruzione superiore e l'integrazione professionale, il che dava adito a conflitti di lealtà. Le questioni pratiche concernenti il sistema informativo di "*Parcoursup*" venivano trattate nel corso di riunioni settimanali. Benché tale forma di organizzazione avesse il vantaggio di tempi di reazione rapidi nella gestione quotidiana dei flussi di studenti, da un punto di vista strategico lasciava "*Parcoursup*" alla deriva.

Infine, il sistema non era abbastanza trasparente. Non consentiva di utilizzare al meglio i dati archiviati sulla piattaforma, nonostante il loro enorme potenziale. Se si fosse sfruttato tale potenziale, si sarebbero potuti ottenere quasi certamente miglioramenti in termini di performance.

Conclusioni e raccomandazioni

Il governo era riuscito a centralizzare l'accesso agli studi post-secondari grazie a una piattaforma digitale che combinava tutti i programmi formativi, in modo da gestire la generalizzazione dell'istruzione superiore. Il sistema precedente era stato affrettatamente rielaborato e trasformato in "*Parcoursup*", senza apportare modifiche strutturali di rilievo. Pertanto, non era stato posto rimedio alle vulnerabilità del sistema informativo in termini di sicurezza, performance e solidità, benché il maggior carico fosse destinato a continuare dato il fine ultimo di includere tutti i corsi di laurea di primo livello. Il sistema era poi documentato inadeguatamente, con un approccio in certa misura artigianale allo sviluppo informatico, e la sua inconsueta complessità aggravava il rischio di errori in caso di modifiche operative. La piattaforma era pertanto esposta a gravi rischi in termini di qualità e continuità dei servizi pubblici e di sicurezza dei dati personali.

La *Cour des comptes* ha formulato le seguenti raccomandazioni:

- sarebbe opportuno aumentare il personale dell'équipe IT dell'SCN e reindirizzare i finanziamenti ORE per incrementare le risorse umane e finanziarie della sottodirezione per i sistemi informativi e la ricerca statistica;

- il sistema informativo dovrebbe essere consolidato per il lungo periodo, correggendone i difetti più evidenti, modernizzandone o rielaborandone l'architettura e documentando le banche dati primarie del vecchio sistema e di "*Parcoursup*" in modo sistematico e strutturato;
- il sistema informativo di "*Parcoursup*" dovrebbe essere dotato di una politica di sicurezza;
- sarebbe opportuno istituire un organismo direttivo congiunto che consenta al ministero dell'Istruzione e della gioventù e al ministero dell'Istruzione superiore, della ricerca e dell'innovazione di vigilare sulla piattaforma "*Parcoursup*", ridistribuendo le risorse dai finanziamenti ORE alle attività di "orientamento".

Lettonia
Valsts Kontrole

La pubblica amministrazione ha sfruttato tutte le opportunità per gestire in maniera efficiente le infrastrutture TIC?

Data di pubblicazione: Giugno 2019

Link alla relazione: Sintesi della relazione (versione inglese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2017-2019

Sintesi della relazione:

Tema dell'audit

L'istituzione superiore di controllo statale della Lettonia ha portato a termine un controllo di gestione sull'efficienza delle infrastrutture TIC pubbliche. L'audit si proponeva di verificare se l'amministrazione pubblica si fosse dotata di un approccio unificato alla gestione efficiente delle infrastrutture TIC e se le istituzioni avessero valutato i benefici della centralizzazione. Inoltre, la sicurezza dei centri dati è stata identificata come importante elemento per valutare le possibilità di un'ulteriore pianificazione dell'ottimizzazione.

La riluttanza delle autorità a gestire le infrastrutture TIC a livello centrale, almeno a livello di un ministero, aveva portato a predisporre una serie di locali server, con un sensibile incremento dei costi di manutenzione. Nei quattro ministeri sottoposti a audit, si è rilevato che le 22 sotto-entità utilizzavano 38 centri dati. Nel corso dell'audit, l'istituzione superiore di controllo ha constatato situazioni in cui sistemi informativi di importanza notevole, persino di livello nazionale, erano ospitati in locali con un livello di sicurezza insufficiente. Ottimizzando il numero dei locali server si potrebbe non solo ridurre le spese relative alle TIC, ma anche ottenere un adeguato livello di sicurezza a

un costo inferiore. Nel frattempo, presso le istituzioni erano già disponibili locali server ad elevato livello di sicurezza, ma non erano utilizzati a piena capacità.

Principale oggetto dell'audit

L'audit si proponeva di verificare che fossero stati creati e attuati tutti i prerequisiti per la gestione unificata delle infrastrutture TIC, in modo da promuovere un uso più efficiente e sicuro delle risorse TIC.

Constatazioni e conclusioni

Governance e ottimizzazione delle TIC

- È mancata, sia a livello nazionale che nei ministeri, una visione a lungo termine dello sviluppo e dell'ottimizzazione delle TIC. I ministeri e le loro sotto-entità hanno ottimizzato le infrastrutture TIC secondo la propria interpretazione e capacità.

Fra il 2011 e il 2017 i costi di manutenzione totali relativi alle TIC delle istituzioni sottoposte a audit sono saliti da 17 a 20 milioni di euro all'anno. Non è stata introdotta alcuna prassi per lo svolgimento di valutazioni periodiche da parte delle istituzioni, per verificare se fosse più economico eseguire la manutenzione dell'infrastruttura TIC internamente, cooperare con un'altra istituzione oppure esternalizzarla. Né la centralizzazione né la decentralizzazione delle TIC sono considerate un obiettivo in sé, ma occorre un'analisi della situazione specifica e delle alternative per fare chiarezza sui costi esistenti e sulle alternative possibili.

Sicurezza delle TIC

- Il quadro giuridico non definiva chiaramente i requisiti di sicurezza delle infrastrutture TIC entro un sistema logico basato sulla pertinenza delle informazioni da trattare. Non erano stati definiti requisiti tecnici dettagliati per la protezione dei centri dati TIC.

- Le carenze relative ai requisiti di sicurezza hanno fatto sì che il costo della protezione fosse elevato o che, al contrario, non fosse assicurata la protezione di informazioni di importanza nazionale. Sistemi di importanza nazionale sono stati persino ospitati in centri dati a bassa sicurezza.

- La maggior parte dei locali server era esposta a minacce alla sicurezza: i centri dati non erano protetti in maniera adeguata dall'accesso fisico né da rischi ambientali. Per la prevenzione delle minacce alla sicurezza occorreva almeno un importo compreso tra i 247 000 e i 765 000 euro, a seconda dell'approccio scelto. Ciò comprendeva: 1) il miglioramento dei locali server contenenti sistemi informatici più importanti e la conservazione di significative risorse TIC in centri dati con un più elevato livello di sicurezza; oppure 2) il miglioramento di tutti i locali server esistenti. Ciò richiederebbe però investimenti di un ammontare che gli auditor non potrebbero giustificare a meno che il numero dei centri dati non venisse ridotto al minimo.

Il quadro giuridico era incompleto poiché non esistevano requisiti di sicurezza dettagliati relativi alle infrastrutture TIC. Ad esempio, esistevano requisiti per i vari criteri relativi alla sicurezza logica, ma non vi era alcun criterio per la sicurezza fisica e ambientale delle infrastrutture, che ha anch'essa un'incidenza sulla disponibilità dei sistemi e sulla protezione dei dati. Benché i documenti relativi alla pianificazione delle politiche pubbliche sottolineassero l'importanza della sicurezza delle infrastrutture TIC e la necessità di rafforzarla, nessuno aveva programmato attività specifiche in questo campo. L'assenza di una differenziazione chiara, tracciabile e logica dei requisiti di sicurezza comportava il rischio che tali requisiti per il trattamento di informazioni di importanza e significato analoghi variassero tra le varie parti del paese.

La sicurezza dello spazio digitale era monitorata dallo Stato a livello centrale, e lo Stato rispondeva agli incidenti che avvenivano a tale livello; la responsabilità della sicurezza delle infrastrutture informatiche era però lasciata al dirigente di ciascuna istituzione. Pertanto la comprensione, da parte delle istituzioni, dei problemi di sicurezza relativi alle TIC, la valutazione dell'importanza delle informazioni trattate e le risorse disponibili alle istituzioni per affrontare i problemi di sicurezza delle TIC differivano notevolmente.

Occorreva pertanto un sistema di monitoraggio periodico di tali processi, in modo da valutare l'intera amministrazione pubblica come sistema unico, in maniera indipendente e secondo criteri standard, identificare approcci diversi e prevenirli individuando i rischi comuni, nonché pianificare azioni preventive tese ad attenuare i rischi.

Lituania
Valstybės Kontrolė

Gestione delle risorse informative statali critiche

Data di pubblicazione: Giugno 2018

Link alla relazione: Sintesi della relazione (versione inglese)
Relazione (versione lituana)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2014-2017

Sintesi della relazione

Tema dell'audit

Con l'uso di risorse informative statali critiche (informazioni elettroniche critiche) si assolvono importanti funzioni pubbliche, come la gestione delle finanze pubbliche, l'amministrazione fiscale e l'assistenza sanitaria. Qualsiasi perdita di informazioni critiche o l'indisponibilità dei corrispondenti sistemi informativi potrebbero avere gravi ripercussioni sulla sicurezza pubblica, il benessere e l'economia. Le valutazioni del controllo informatico generale effettuate dall'Ufficio nazionale di audit della Lituania dal 2006 al 2016 hanno rivelato problemi ricorrenti nella gestione informatica (pianificazione, definizione dell'architettura informativa, struttura organizzativa, modifiche, garanzia della continuità operativa, sicurezza dei dati, monitoraggio e valutazione della gestione informatica). L'Ufficio ha svolto un audit sulle risorse informative statali critiche per valutare la gestione e la sicurezza di tali risorse e per offrire misure di miglioramento.

L'audit si proponeva di valutare la gestione (controllo generale) e la maturità delle risorse informative statali critiche, nonché di identificare i problemi sistemici.

L'Ufficio ha valutato la maturità della gestione informatica in 12 organizzazioni del settore pubblico[64] che amministrano 44 sistemi informativi statali di prima classe. L'audit è stato effettuato secondo i requisiti relativi all'audit del settore pubblico e i princìpi internazionali delle istituzioni superiori di controllo. La valutazione è stata effettuata secondo la metodologia COBIT[65] nei seguenti settori a maggior rischio: pianificazione strategica informatica; determinazione dell'architettura informativa; gestione del rischio informatico; gestione delle modifiche; garanzia della continuità nella fornitura dei servizi; sicurezza dei sistemi; gestione dei dati; monitoraggio e valutazione delle attività informatiche; garanzia della gestione informatica. La valutazione del processo comprendeva sia la gestione informatica organizzativa e nazionale, sia l'interazione fra questi livelli di gestione.

Constatazioni di audit

Le tendenze rilevate nei cambiamenti del livello di maturità per quanto riguarda la gestione delle risorse informative statali critiche erano positive. Alla luce del crescente livello di ciberminacce, i progressi registrati erano tuttavia troppo lenti ed era necessario incrementare la sicurezza di queste risorse, in considerazione delle seguenti debolezze:

- il sistema per individuare le risorse informative statali critiche non si è dimostrato sufficientemente efficace da consentire l'attuazione di soluzioni di sicurezza tali da soddisfare le effettive esigenze:
  - le valutazioni intese a dimostrare la criticità delle risorse informative statali mancavano di obiettività, i cambiamenti non venivano sempre valutati in sede di riesame, questo processo non era monitorato a livello nazionale e gli orientamenti per la definizione delle criticità non garantivano un'attuazione efficace;

[64] Ispettorato nazionale delle imposte, centro dei registri delle imprese pubbliche, dipartimento delle tecnologie dell'informazione e della comunicazione (TIC), comitato del fondo statale di previdenza sociale, impresa di Stato "Centro d'informazione agricola e di economia rurale", centro del sistema informativo doganale, servizio alimentare e veterinario statale, ufficio del *Seimas* della Repubblica di Lituania, ministero delle Finanze, commissione per lo sviluppo della società dell'informazione, fondo statale per i pazienti, servizio forestale statale.

[65] COBIT è un modello dell'organizzazione internazionale ISACA che definisce le migliori pratiche per la gestione informatica.

— il sistema per individuare le risorse informative statali critiche e le infrastrutture informative critiche non era standardizzato; risorse e infrastrutture venivano individuate diversamente a seconda dell'importanza delle informazioni e dei servizi, complicando in tal modo il processo di individuazione di tali risorse;

— non era stata sviluppata un'architettura informativa nazionale per rappresentare i sistemi informativi statali e le loro interrelazioni, per indicare l'entità delle risorse informative statali critiche e per consentire di adottare decisioni informate in merito all'importanza di tali risorse.

o La gestione delle risorse informative statali doveva essere maggiormente in linea con le migliori pratiche e norme di gestione informatica, per ottenere un miglioramento integrato nel settore informatico, così da contribuire a progressi più marcati nella gestione delle risorse informative statali critiche:

— la pianificazione informatica non era sostenibile: gli strumenti informatici programmati venivano presentati in documenti differenti, mancava un approccio sistematico a causa del numero eccessivo di documenti strategici, che rendeva difficile individuare le priorità essenziali e incanalare risorse verso la gestione delle minacce più gravi;

— il monitoraggio informatico non garantiva che le organizzazioni misurassero l'efficienza delle operazioni informatiche e che gli audit svolti dai dirigenti responsabili delle risorse informative statali critiche indicassero la reale maturità della gestione informatica. La gestione informatica statale non veniva esaminata a livello nazionale e i relativi problemi non venivano analizzati in modo sistematico. Era stato creato un sistema per monitorare la conformità delle risorse informative statali ai requisiti di sicurezza delle informazioni elettroniche, volto unicamente ad agevolare il monitoraggio del rispetto della sicurezza, ma le sue funzionalità non erano utilizzate abbastanza.

o Le misure adottate per garantire una resilienza delle risorse informative critiche commisurata al livello delle minacce informatiche non erano sufficientemente efficaci; per tali risorse permaneva quindi un rischio di vulnerabilità:

— era necessario rendere più efficace la valutazione dei rischi per la sicurezza informatica, poiché non erano stati individuati tutti i rischi pertinenti e la metodologia per la loro valutazione non era conforme alle più recenti

pratiche di gestione informatica; non veniva assicurata una gestione tempestiva dei rischi inaccettabili;

— non venivano sistematicamente adottate misure di sicurezza organizzativa in grado di attenuare le ciberminacce. Test di sicurezza insufficienti, formazione incompleta del personale durante lo sviluppo, l'aggiornamento e la modifica del sistema informativo; mancata gestione di configurazioni e aggiornamenti sicuri del software; gestione scorretta della continuità dell'attività informatica e dei file di back-up minacciavano la continuità operativa delle imprese; le misurazioni della performance in materia di sicurezza erano insufficienti e non contribuivano a rafforzare la sicurezza.

Conclusioni

In media, la gestione informatica degli enti del settore pubblico sottoposti ad audit negli ultimi dieci anni ha raggiunto il primo livello di maturità su una scala di cinque[66] e si collocava a un livello di 1,7 nel momento in cui è stato redatto questo documento. Questo modesto livello di maturità delle risorse informative statali critiche rivelava debolezze nella formulazione e nell'attuazione della politica per le risorse informative statali, il che aumentava la vulnerabilità delle risorse stesse. Per rafforzare la sicurezza di tali risorse, occorre migliorare il meccanismo di gestione delle risorse informative statali per adeguarlo alle migliori pratiche, nella misura del possibile. Gli auditor hanno inoltre rilevato che le misure tese ad assicurare la resistenza delle risorse informative critiche alle ciberminacce non erano abbastanza efficaci. È pertanto necessario rendere più efficace la valutazione dei rischi per la sicurezza informatica, dando maggiore importanza ai test di sicurezza al momento di elaborare e modernizzare i sistemi informativi e di formare il personale.

[66] Secondo la metodologia COBIT.

Altre relazioni in questo settore

Titolo della relazione:	Il contrasto alla cibercriminalità è efficace?
Link alla relazione:	Sintesi della relazione (versione inglese) Relazione (versione lituana)
Data di pubblicazione:	2020

Titolo della relazione:	L’ambiente della cibersicurezza in Lituania
Link alla relazione:	Sintesi della relazione (versione inglese) Relazione (versione lituana)
Data di pubblicazione:	2015

Ungheria
Ufficio statale di audit

Audit sulla protezione dei dati – Audit sul quadro nazionale per la protezione dei dati e su taluni registri di dati prioritari nel quadro della cooperazione internazionale

Data di pubblicazione: Marzo 2017

Link alla relazione: Relazione (versione ungherese)

Tipo e periodo dell'audit

Tipo di audit: Audit di conformità

Periodo sottoposto ad audit: 2011-2015

Sintesi della relazione

Tema dell'audit

La sicurezza del patrimonio nazionale di dati rappresenta in ogni paese un fondamentale interesse della società per la conservazione e la tutela dei valori nazionali. Di conseguenza, per consolidare la fiducia dei cittadini nello Stato e assicurare il costante e corretto funzionamento dell'amministrazione pubblica è essenziale potenziare la sicurezza dei dati personali e pubblici nell'ambito del patrimonio nazionale di dati dell'Ungheria. La protezione dei dati e la rete di sicurezza offerta dal quadro giuridico per la sua applicazione rivestono pertanto un'importanza cruciale per la società.

Nel settore della protezione dei dati, l'amministrazione pubblica svolge un ruolo chiave nella gestione dei registri di dati più voluminosi e sensibili appartenenti al patrimonio nazionale di dati. I titolari del trattamento dei dati per i registri operano in stretta collaborazione nello svolgimento delle proprie mansioni. Trasferiscono periodicamente i registri contenenti grandi quantità di dati e devono seguire con grande attenzione le prescrizioni di legge in materia di protezione dei dati. Oggi l'uso dei sistemi informativi elettronici per gestire e trattare i dati è essenziale; occorre quindi garantire il

funzionamento adeguato e affidabile dei sistemi effettuando controlli opportunamente concepiti ed eseguiti.

Nel corso degli audit l'Ufficio statale di audit ungherese riserva grande attenzione alla protezione dei dati. Tra il 2011 e il 2015 ha espletato audit esaustivi in merito alla protezione dei dati, a seguito dei quali ha redatto una relazione nel primo trimestre del 2017. Sono stati trattati anche aspetti di audit internazionali svolti parallelamente in cooperazione con il gruppo di lavoro EUROSAI sulle tecnologie dell'informazione, che riguardavano principalmente la conformità alle vigenti direttive dell'Unione europea.

L'audit di conformità sulla protezione dei dati in Ungheria si prefiggeva l'obiettivo di valutare se nel paese fosse stato istituito un quadro normativo e operativo per la protezione dei dati e se le più importanti organizzazioni di gestione dei dati avessero rispettato le prescrizioni per la gestione sicura dei dati e l'esternalizzazione del trattamento dei dati. L'audit si è incentrato in particolare sulla protezione dei dati personali e del patrimonio nazionale di dati.

Nel contesto dell'audit l'Ufficio statale di audit ha valutato la gestione dei dati in sei organizzazioni preposte alla gestione dei dati (per esempio: autorità fiscale, tesoro nazionale, assicurazione sanitaria, pagamento delle pensioni, ufficio istruzione, indirizzi e dati personali, registri di veicoli e viaggi, agenzie amministrative per la gestione dei dati del casellario giudiziario), nonché le attività dell'autorità per la protezione dei dati e dell'autorità per la sicurezza delle informazioni.

L'audit ha prestato particolare attenzione al mandato delle organizzazioni preposte alla gestione dei dati, in particolare nel caso di trasferimento di dati a terzi. Durante l'audit dei controlli interni sulla gestione e il trattamento dei dati è stata valutata l'esistenza di una regolamentazione aggiornata in materia di doveri, responsabilità e competenze, gestione e processi relativi alle risorse umane.

Per quanto riguarda i sistemi elettronici utilizzati nella gestione dei dati, l'Ufficio statale di audit ha valutato le relative misure di sicurezza, tra cui le aree di protezione fisica, i diritti di accesso, la registrazione, le procedure per la valutazione della sicurezza, la sicurezza dei sistemi e delle comunicazioni, nonché il rispetto della classificazione della sicurezza dell'organizzazione nel suo complesso.

L'esternalizzazione del trattamento dei dati è stata controllata sulla base dei contratti conclusi, verificando se le organizzazioni responsabili della gestione dei dati

obbligassero le organizzazioni per il loro trattamento a rispettare i requisiti connessi alle attività di trattamento dei dati conformemente alla disciplina legislativa.

Constatazioni e conclusioni

Sulla base dell'audit, l'Ufficio statale di audit ungherese ha rilevato che le norme interne delle organizzazioni di gestione dei dati in materia di attività di gestione dei dati garantivano la protezione del patrimonio nazionale di dati nell'ambito del patrimonio nazionale, conformemente alle disposizioni giuridiche vigenti fra il 2011 e il 2015. In pratica, i titolari del trattamento dei dati hanno applicato correttamente i requisiti per la gestione sicura dei dati e l'esternalizzazione del trattamento dei dati. Il trasferimento di dati a terzi è stato attuato ai sensi del mandato appropriato e di una chiara definizione delle responsabilità e dei poteri.

Per alcuni titolari del trattamento dei dati è risultato che la classificazione della sicurezza dei sistemi elettronici e dell'organizzazione nel suo complesso non era sempre conforme ai requisiti di legge, ma l'entità delle carenze non comprometteva in maniera sostanziale la sicurezza dei dati trattati. Sulla base delle raccomandazioni incluse nella relazione di audit, le organizzazioni competenti per la gestione dei dati hanno posto rimedio alle carenze nel quadro di piani di azione approvati dall'Ufficio statale di audit.

Per quanto riguarda l'audit internazionale svolto parallelamente in cooperazione con il gruppo di lavoro EUROSAI sulle tecnologie dell'informazione, l'Ufficio statale di audit ha constatato che la legislazione ungherese in materia di protezione dei dati era conforme alla vigente direttiva dell'UE.

In conclusione, con l'audit sulla protezione dei dati l'Ufficio statale di audit ungherese ha contribuito alla buona governance e alla protezione del patrimonio nazionale dei dati.

Altre relazioni in questo settore

Titolo della relazione:	Relazione – Audit di monitoraggio sul seguito dato – Audit sulla protezione dei dati – Audit sul quadro nazionale per la protezione dei dati e su taluni registri di dati prioritari nel quadro della cooperazione internazionale
Link alla relazione:	Relazione (versione ungherese)
Data di pubblicazione:	2020

Paesi Bassi
Corte dei conti

Cibersicurezza delle strutture critiche di gestione idrica e dei controlli di frontiera nei Paesi Bassi

Date di pubblicazione: Marzo 2019 e aprile 2020

Link alle relazioni: Sintesi della relazione concernente la cibersicurezza e le strutture idriche critiche – Relazione (versione inglese)

Sintesi della relazione concernente la cibersicurezza e i controlli automatizzati alle frontiere – Relazione (versione inglese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2018-2020

Sintesi della relazione

Tema dell'audit

Nel 2018 la Corte dei conti dei Paesi Bassi ha deciso di effettuare audit sulla cibersicurezza in settori di importanza cruciale per la società. Sulla base di una lunga esperienza di audit sul rispetto della sicurezza delle informazioni nell'amministrazione centrale, la Corte dei conti ha ritenuto che audit incentrati sulla *performance* delle politiche e delle misure nella pratica potessero recare un valore aggiunto. Anzitutto sono stati sottoposti ad audit la gestione idrica e i controlli automatizzati alle frontiere: la prima è vitale per una nazione situata in gran parte al di sotto del livello del mare, mentre i secondi sono essenziali in ragione della condizione dell'aeroporto di Schiphol Amsterdam quale *hub* internazionale e porta d'ingresso nel paese.

Il ministro delle Infrastrutture e della gestione idrica ha indicato come "elementi critici" del settore della gestione idrica una serie di strutture idriche gestite dalla direzione generale dei lavori pubblici e della gestione idrica (il soggetto controllato).

Molti sistemi informatici utilizzati per il funzionamento delle strutture idriche critiche risalgono agli anni ottanta e novanta, quando generalmente non si teneva conto della cibersicurezza. Tali sistemi erano stati originariamente concepiti come sistemi a sé stanti, ma gradualmente sono stati collegati a reti informatiche di dimensioni maggiori, per esempio allo scopo di facilitare il funzionamento a distanza. Tale tendenza ha reso i sistemi più vulnerabili alle ciberminacce.

Il ministro della Difesa e il ministro della Giustizia e della sicurezza condividono la responsabilità dei controlli di frontiera effettuati dalle guardie di frontiera neerlandesi all'aeroporto di Schiphol. Entrambi i ministeri (i soggetti controllati) dispongono di sistemi informatici utilizzati dalle guardie di frontiera. Tali sistemi sono essenziali per le operazioni aeroportuali e vengono impiegati per trattare dati altamente sensibili. Costituiscono di conseguenza un ambìto obiettivo per i ciberattacchi sferrati a fini di sabotaggio, spionaggio o manipolazione dei controlli di frontiera.

Si è verificato in che modo i soggetti controllati fossero preparati a trattare le ciberminacce e se ciò avvenisse in modo efficace.

- I quesiti di audit si proponevano di dare una risposta ai seguenti interrogativi. In che modo i soggetti controllati *proteggono* i sistemi dalle ciberminacce e *prevengono* i ciberattacchi?
- In che modo i soggetti controllati *individuano* le ciberminacce e i ciberattacchi?
- In che modo i soggetti controllati *reagiscono* qualora si verifichi un ciberattacco?

Entrambi gli audit hanno dato particolare rilievo all'efficacia. In stretta collaborazione con i soggetti controllati, hacker etici hanno operato sulle strutture idriche critiche e su uno dei sistemi di controllo alle frontiere. Ovviamente, tutte le constatazioni emerse dalle verifiche sono state affrontate prima che le relazioni fossero pubblicate e non è stato divulgato alcun particolare tecnico.

La principale differenza fra i due audit risiede nel fatto che l'audit sulle strutture idriche si è concentrato sul conseguimento degli obiettivi del soggetto controllato, mentre l'audit sui controlli alle frontiere si è basato sul quadro di cibersicurezza NIST.

Constatazioni

In primo luogo, da entrambi gli audit è emerso che i soggetti controllati erano consapevoli delle ciberminacce e stavano già applicando un approccio professionale al problema.

Per quanto riguarda le strutture idriche, tuttavia, il soggetto controllato doveva intensificare ulteriormente gli sforzi di individuazione e risposta, per rispettare i propri obiettivi in materia di cibersicurezza. Il soggetto controllato aveva istituito un centro delle operazioni di sicurezza (SOC) per individuare i ciberattacchi e rispondervi. Tuttavia, nell'autunno del 2018 non era ancora stato conseguito l'obiettivo, fissato per la fine del 2017, di individuare istantaneamente qualsiasi ciberattacco diretto contro le strutture idriche critiche. Di conseguenza, un ciberattacco diretto contro una struttura idrica critica rischiava di non essere individuato o di esserlo troppo tardi. Per di più la verifica condotta presso una delle strutture idriche critiche ha dimostrato che era possibile accedervi fisicamente. Gli hacker sono riusciti ad accedere alla sala di controllo e si sono ritrovati da soli di fronte a stazioni di lavoro prive di protezione. Infine il soggetto controllato non aveva predisposto scenari per una crisi provocata da un ciberattacco e le informazioni relative alla risposta mancavano o non erano aggiornate. La presenza di informazioni aggiornate potrebbe rivelarsi cruciale per una risposta rapida ed efficace a una situazione di crisi.

Per quanto riguarda i controlli alla frontiera, si è constatato che le misure di cibersicurezza non erano né appropriate né adatte alle sfide del futuro. In primo luogo, importanti sistemi di controllo alle frontiere dovevano essere approvati formalmente prima di iniziare a operare, per far sì che tutte le misure di cibersicurezza fossero attuate. Si è constatato che due sistemi su tre operavano senza approvazione: in altre parole, non vi era alcuna garanzia che le misure di sicurezza necessarie fossero in atto. In secondo luogo, un SOC era operativo, ma nessuno dei sistemi vi era collegato direttamente. Sebbene un'infrastruttura generica fosse collegata al SOC, ciò non escludeva ancora il rischio che un ciberattacco passasse inosservato o fosse scoperto in ritardo. In terzo luogo le verifiche della sicurezza non venivano effettuate con regolarità. Soltanto uno dei tre sistemi era stato testato in passato, e solo in misura limitata. Infine, come per il primo audit, non era stato elaborato uno scenario specifico per una crisi provocata da un ciberattacco.

Nel corso delle verifiche della sicurezza di uno dei sistemi mai testati in precedenza, gli hacker etici hanno rilevato una serie di vulnerabilità che, se combinate, potevano essere sfruttate da un insider malevolo non autorizzato per sferrare un ciberattacco e accedere a informazioni nel sistema, copiarle e persino manipolarle. Tali risultanze dimostrano quanto sia importante effettuare verifiche periodiche della sicurezza.

Le constatazioni sono preoccupanti alla luce dell'automazione dei processi di frontiera che è attualmente in corso. Nel prossimo futuro un numero crescente di sistemi di controlli di frontiera tratterà un numero sempre maggiore di dati usando un numero

crescente di connessioni. Ciò accresce il rischio di ciberattacchi e, di conseguenza, l'approccio adottato non poteva essere considerato idoneo a rispondere alle sfide future.

Conclusioni

Nel caso delle strutture idriche alcuni elementi essenziali hanno impedito al soggetto controllato di adottare le misure di cibersicurezza finali. Non era chiaro, per esempio, quale fosse il livello delle minacce ed era pertanto difficile valutare se le misure adottate e la dotazione finanziaria assegnata fossero sufficienti. Inoltre, il dipartimento centrale responsabile della cibersicurezza non aveva il mandato per attuare le misure di cibersicurezza necessarie presso le strutture idriche decentralizzate. Le raccomandazioni di audit su questo punto sono state seguite, consentendo all'organizzazione di progredire.

Per quanto riguarda i controlli alla frontiera, non si è individuato un motivo chiaro per il livello insufficiente di cibersicurezza. Le ricerche condotte nell'ambito dell'audit hanno rilevato strategie e procedure di cibersicurezza complete e dettagliate, competenze adeguate e dipendenti qualificati. Le raccomandazioni di audit, pertanto, miravano soprattutto a far sì che venisse adottata ogni misura possibile.

Entrambi gli audit hanno suscitato la viva attenzione del parlamento e dei media, svolgendo un'opera di sensibilizzazione sulla cibersicurezza delle infrastrutture critiche e offrendo spunti ai soggetti controllati sui possibili modi per accrescere la cibersicurezza. Si è rivelata essenziale una stretta collaborazione con i soggetti controllati per comprenderne a fondo la situazione, affrontare i rischi dell'indagine e verificare la cibersicurezza.

È anche in programma un terzo audit di questa stessa serie. Inoltre il livello di sicurezza delle informazioni del governo nazionale dei Paesi Bassi costituisce un elemento fondamentale del ciclo annuale di audit di conformità. Nel corso degli anni, l'ISC neerlandese ha constatato che, per quanto riguarda le misure volte a garantire la sicurezza delle informazioni, molti ministeri non hanno un livello adeguato. La Corte dei conti sfrutta attualmente l'esperienza acquisita con gli audit sulla cibersicurezza per ampliare le prospettive degli audit sulla sicurezza delle informazioni, spingendosi oltre l'esame di strategie e documenti per verificare la reale efficacia delle misure.

Altre relazioni in questo settore

Titolo della relazione: Capitolo 3 di “Staat van de rijksverantwoording 2019”

Link alla relazione: Relazione (versione neerlandese)

Data di pubblicazione: 2020

Titolo della relazione: Telelavoro digitale

Link alla relazione: Relazione (versione neerlandese)

Data di pubblicazione: 2020

Polonia
Najwyższa Izba Kontroli

Garantire la sicurezza del funzionamento dei sistemi informatici utilizzati per assolvere funzioni pubbliche

Data di pubblicazione: 2016

Link alla relazione: Relazione (versione polacca)

Tipo e periodo dell'audit

Tipo di audit: Audit di conformità

Periodo di audit: 2014-2015

Sintesi della relazione

Tema dell'audit

L'audit era teso a valutare se i dati raccolti nei sistemi destinati ad assolvere importanti funzioni pubbliche fossero sicuri nelle unità sottoposte a audit. L'audit ha interessato sei istituzioni selezionate che assolvevano rilevanti funzioni pubbliche. Previa analisi, in ognuna delle istituzioni è stato selezionato un sistema informatico che poi è stato esaminato nel dettaglio. Per l'audit è stata utilizzata la versione 4.1 del metodo COBIT (obiettivi di controllo nel campo dell'informazione e delle tecnologie correlate).

L'audit è stato effettuato sulla scia dell'audit del 2015 sulla performance degli organismi pubblici polacchi in materia di cibersicurezza[67], nelle cui constatazioni erano segnalati problemi sistemici. L'audit del 2016 ha dimostrato tra l'altro che fino a quel momento l'amministrazione statale non aveva agito per garantire la sicurezza informatica a livello nazionale. Si è giunti alla conclusione che le attività degli organismi pubblici per la protezione del ciberspazio si sono svolte in maniera frammentaria, senza un approccio sistematico. In assenza di disposizioni a livello centrale, tali da garantire concrete condizioni di sicurezza per specifici sistemi informatici essenziali al

[67] https://www.nik.gov.pl/kontrole/P/14/043/

funzionamento dello Stato, l'audit ha cercato di esaminare se le istituzioni che amministrano i sistemi informatici usati per assolvere importanti funzioni pubbliche garantissero lo svolgimento in sicurezza di tali funzioni.

Nel 2019 è stato approvato un altro audit dei sistemi incentrato sulla cibersicurezza, dal titolo "La cibersicurezza in Polonia", ma le constatazioni sono riservate.

Quesiti di audit

I sotto-obiettivi sono suddivisi in due aree di valutazione, che intendono rispondere a quesiti specifici.

Per quanto riguarda il sostegno alla sicurezza informatica, a livello dell'intera organizzazione l'audit ha esaminato tra l'altro se:

- si attuasse la gestione della sicurezza informatica;
- si applicassero piani per garantire la sicurezza informatica;
- la sicurezza informatica fosse oggetto di verifiche, supervisione e monitoraggio;
- fossero definiti gli incidenti di sicurezza informatica;
- la gestione informatica avvenisse tramite chiavi crittografiche;
- si operasse per individuare i software malevoli, proteggersene e installare patch;
- si garantisse la sicurezza della rete.

Per quanto riguarda il sostegno alla sicurezza, l'audit ha tra l'altro esaminato a livello dei sistemi selezionati se:

- venissero gestiti l'identità e gli account degli utenti;
- venissero protetti i dati sensibili e le tecnologie per la sicurezza.

Constatazioni e conclusioni

Il grado di preparazione e attuazione del sistema di sicurezza delle informazioni non ha garantito un livello di sicurezza accettabile per i dati raccolti nei sistemi informatici deputati a svolgere importanti funzioni pubbliche. I processi di sicurezza delle informazioni si svolgevano in maniera disordinata e, in mancanza di procedure, intuitiva. Tra le sei unità sottoposte a audit, soltanto una aveva attuato il sistema di

sicurezza delle informazioni, e si deve osservare che anche il suo funzionamento era inficiato da gravi debolezze. In tutte le unità sottoposte ad audit, tranne una, i lavori per garantire condizioni di sicurezza adeguate per le informazioni trattate nei sistemi informatici non avevano raggiunto un livello soddisfacente perché, iniziati solo di recente, si trovavano ancora nella fase preliminare, in cui rientrava anche la preparazione delle necessarie basi formali. Essi si fondavano su disposizioni semplificate o informali, tratte dalle buone pratiche o dall'esperienza maturata dal personale informatico fino ad allora.

Conformemente alla metodologia COBIT 4.1, la maturità del processo di gestione della sicurezza delle informazioni nelle unità sottoposte ad audit variava da (1) iniziale/ad hoc a (3) definita, su una scala da zero a cinque, in cui cinque è il punteggio massimo.

La responsabilità di garantire la sicurezza informatica nelle unità sottoposte ad audit spettava al coordinatore della sicurezza, che però, di fatto, non era competente per la gestione dell'intero processo. Inoltre le funzioni interessate erano spesso svolte da una sola persona. Benché fossero stati nominati gruppi di specialisti o fossero stati conclusi accordi con contraenti esterni, non era stata effettuata l'analisi necessaria per stabilire se i servizi forniti soddisfacessero le esigenze di sicurezza dell'unità. Le unità controllate avevano una comprensione frammentaria e limitata dell'esigenza di garantire la sicurezza informatica. La sicurezza dei dati era considerata essenzialmente responsabilità e competenza del dipartimento informatico e non di tutte le unità organizzative con compiti previsti per legge; ciò ostacolava notevolmente lo sviluppo di sistemi di sicurezza informatica coerenti e validi per l'intera istituzione.

Se si mette a confronto il modo in cui gli obblighi di garantire la sicurezza delle informazioni venivano rispettati nel complesso delle organizzazioni e nei sistemi selezionati, risulta evidente che la qualità dell'attuazione era più elevata nel secondo caso. La causa è forse da ricercarsi nell'impatto che le conoscenze pratiche e il coinvolgimento del personale tecnico di medio livello avevano sulla sicurezza, nel maggior impiego all'interno della pubblica amministrazione di sistemi informatici commerciali basati su standard di mercato e nelle soluzioni avanzate di garanzia della sicurezza. Applicando tali soluzioni, l'esperienza acquisita e le buone pratiche, è stato possibile mantenere un determinato livello di sicurezza nel funzionamento dei vari sistemi anche in condizioni di risorse limitate, carenze organizzative o regolamentazione "disfunzionale". Questa non può essere però una soluzione definitiva; infatti, in un periodo di dinamico incremento del livello delle minacce, la sicurezza dei sistemi informatici non può fondarsi su misure gestite in maniera disordinata e intese solamente a superare le difficoltà più immediate.

Conclusioni di audit

Occorre sviluppare e attuare a livello centrale raccomandazioni generali sulla sicurezza informatica e prescrizioni applicabili a tutti gli enti pubblici. È necessario individuare una soluzione sistemica con cui divulgare le risultanze degli audit sulla sicurezza informatica, in modo da consentire ai cittadini di accedere alle informazioni sulle attività degli enti pubblici, mantenendo invece limitato l'accesso alla conoscenza delle misure e dei metodi usati per garantire la sicurezza delle informazioni trattate.

Altre relazioni in questo settore

Titolo della relazione:	Gestione della sicurezza delle informazioni da parte delle autorità regionali
Link alla relazione:	Relazione (versione polacca)
Data di pubblicazione:	2019

Titolo della relazione:	La cibersicurezza in Polonia (informazioni classificate)
Link alla relazione:	*Non accessibile al pubblico*
Data di approvazione	2019

Titolo della relazione:	Garanzia della sicurezza dei sistemi informatici a opera delle autorità regionali nel voivodato di Podlaskie
Link alla relazione:	Relazione (versione polacca)
Data di pubblicazione:	2018

Titolo della relazione:	Prevenzione e lotta contro il ciberbullismo tra minori e giovani
Link alla relazione:	Relazione (versione polacca)
Data di pubblicazione:	2017

Titolo della relazione:	Svolgimento dei compiti di cibersicurezza da parte degli organismi pubblici in Polonia
Link alla relazione:	Relazione (versione polacca)
Data di pubblicazione:	2015

Titolo della relazione:	Attuazione di prescrizioni selezionate in materia di sistemi informativi, scambio elettronico di informazioni e quadro nazionale di interoperabilità secondo l'esempio di alcuni consigli comunali e città con diritti distrettuali.
Link alla relazione:	Relazione (versione polacca)
Data di pubblicazione:	2015

Portogallo
Tribunal de Contas

Audit sul passaporto elettronico portoghese

Data di pubblicazione: 2014

Link alla relazione: Relazione (versione portoghese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2013

Sintesi della relazione

Tema dell'audit

L'audit operativo del passaporto elettronico portoghese (PEP) era diretto ad accertare l'efficacia dei sistemi informativi su cui si fondano la concessione, il rilascio e l'utilizzo del passaporto, soprattutto per quanto riguarda lo screening automatizzato dei passeggeri tramite lettura dei dati biometrici alle frontiere del Portogallo[68].

I principali obbiettivi dell'audit erano:

- verificare la conformità alla normativa nazionale e dell'UE, alle norme internazionali e agli orientamenti per la concessione, il rilascio e l'utilizzo del PEP, compresa l'adeguatezza del quadro giuridico nazionale;
- esaminare aspetti cruciali della performance dei sistemi informativi, in particolare il rispetto dei requisiti di sicurezza dei sistemi informativi del PEP (SIPEP).

[68] Si tratta dei sistemi di controllo automatizzato alle frontiere (ABC) nell'ambito di Frontex (Agenzia europea della guardia di frontiera e costiera).

Le principali aree di rischio erano le seguenti:

- perdita/furto di beni materiali e/o informazioni elettroniche;
- uso improprio di informazioni riservate;
- rischio di conformità (mancato rispetto delle prescrizioni giuridiche e normative).

Periodo sottoposto ad audit: 1° gennaio 2013-31 dicembre 2013 (se del caso, da estendere ad anni precedenti e successivi).

Constatazioni e conclusioni

Il passaporto elettronico portoghese (PEP) comprende tre categorie: comune[69], diplomatico o speciale. Esiste anche un passaporto per cittadini di altri paesi, che conferisce diritti inferiori.

Il sistema di concessione prevede vari moduli di domanda e vari organismi competenti per la raccolta dei dati e la concessione del passaporto, ma soltanto un ente competente per il rilascio (che racchiude in sé produzione, personalizzazione e consegna).

Diversi enti (enti PEP) partecipano al processo. Gli enti responsabili per la raccolta dei dati e la concessione dei passaporti sono i seguenti:

- Portogallo continentale: il Serviço de Estrangeiros e Fronteiras (SEF)[70] e i servizi anagrafici dell'Instituto dos Registos e do Notariado (IRN)[71];
- Regioni autonome delle Azzorre[72] e di Madera: servizi della rispettiva *Vice-Presidência do Governo Regional*[73]; all'estero: consolati portoghesi;

---

[69] Circa il 99 % del totale.

[70] Servizio per l'immigrazione e le frontiere.

[71] Anagrafe e ufficio notarile (solo ricevimento).

[72] Nonché i centri servizi dell'*Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* – Agenzia per la modernizzazione e la qualità dei servizi al cittadino, istituto pubblico (solo ricevimento).

[73] Vicepresidenza dell'amministrazione regionale.

- The Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] rilascia e consegna i passaporti.

I processi principali si fondano per lo più sul SIPEP (sistema centrale di gestione delle domande per il rilascio dei passaporti portoghesi). Il SIPEP consente di registrare, conservare, trattare, convalidare e fornire le informazioni richieste per la concessione del PEP, avvia il processo di personalizzazione svolto dall'INCM e assicura l'interconnessione con altre applicazioni del sistema, coordinando tutti gli enti PEP partecipanti alla registrazione fisica e logistica dei dati raccolti.

Gli enti PEP hanno una struttura organizzativa che consente loro di realizzare gli obiettivi giuridici associati con il PEP. Per quanto riguarda la domanda e la raccolta, il sistema si fonda ancora in larga misura sulle risorse umane. Il SIPEP comprende però un gran numero di funzioni di trattamento e controlli di convalida automatici.

Dal momento che le procedure prevedono funzioni di controllo e manipolazioni di dati, alcune delle quali si possono svolgere indipendentemente senza l'intervento umano, il SIPEP esercita un impatto significativo in termini di organizzazione e sistema informativo, soprattutto per quanto riguarda: i) la comprensione e la definizione di norme, processi e dati richiesti, e ii) la definizione dei requisiti del sistema informativo.

L'efficienza e l'efficacia del processo di raccolta dei dati sono garantite dall'interazione del SIPEP con altri sistemi informativi[75], conformemente alle norme di legge.

È stato istituito un quadro per il controllo complessivo delle attività informatiche (governance, sviluppo e acquisizione, operazioni informatiche, continuità operativa e ripristino in caso di disastro, sicurezza delle informazioni); seppur non estesamente documentato, esso assicura lo sviluppo, il funzionamento, la gestione e la manutenzione del sistema SIPEP.

Indicatori di attività (2013):

- sono stati concessi circa 500 000 PEP, il 63 % dei quali dal SEF, il 33 % da consolati portoghesi e il 4 % dalle amministrazioni regionali;

[74] Ufficio pubblicazioni nazionali e Zecca, azienda pubblica.

[75] Segnatamente: il sistema informativo integrato del SEF (SIISEF); la sezione nazionale del sistema d'informazione Schengen (NSIS); la banca dati dell'anagrafe, il casellario giudiziario.

- gli introiti derivanti dal rilascio dei PEP sono stati pari a circa 37 milioni di euro, derivanti soprattutto dall'INCM (43 %), dal SEF (32 %) e dal *Ministério dos Negócios Estrangeiros (MNE)*[76] (17 %).

Per il 2013, le verifiche effettuate sul SIPEP non hanno confermato il rispetto del tempo massimo di consegna stabilito per legge (dalla data della domanda al momento della messa a disposizione del PEP presso il punto di consegna) poiché la data effettiva di arrivo presso il punto di consegna non è stata sempre registrata tempestivamente.

Gli investimenti relativi all'acquisizione delle attrezzature per la raccolta dei dati biometrici e della firma (chioschi), delle attrezzature per i sistemi di controllo automatizzati alle frontiere (ABC) e all'acquisizione e alla manutenzione di sistemi, servizi e assistenza tecnica informatici sono stati effettuati da SEF, MNE, RIAC e INCM per un importo di 11 milioni di euro; la somma più alta è stata spesa dal SEF.

Prima del PEP il prezzo del passaporto (non biometrico) della Repubblica portoghese era di 22,44 euro; nel 2006 il PEP comune (biometrico) costava 60 euro, saliti a 65 euro nel 2011.

Domande di PEP

Le domande di PEP sono trattate personalmente dai servizi competenti che ricevono i documenti relativi alla domanda, raccolgono i dati biografici e biometrici del richiedente, riscuotono i diritti e, successivamente, consegnano il PEP dopo il rilascio.

Il sistema su cui si basa il PEP (SIPEP) convalida la correttezza e la qualità dei dati tramite controlli virtuali e riferimenti incrociati con altri sistemi informativi, in particolare la banca dati dell'anagrafe, per verificare che la domanda sia conforme e idonea alla concessione e al rilascio del PEP.

I relativi cambiamenti di stato sono registrati nei file di registro, assicurando così la possibilità di verifica, l'integrità e la non disconoscibilità delle operazioni.

[76] Ministero degli Affari esteri.

La trasmissione dei dati tra gli organismi preposti alla raccolta (in Portogallo e all'estero) e il SEF avviene tramite VPN (rete virtuale privata), in base alla gestione degli accessi conformemente alle credenziali controllate dal SEF[77].

La domanda di PEP comune è trattata in modo diverso qualora sia presentata da cittadini i cui diritti sono soggetti a limitazioni: i) coloro che non possono esercitare i propri diritti (minori, persone incapaci o sottoposte a interdizione giudiziale); ii) persone soggette a interdizione legale o a provvedimenti di polizia (per precedenti penali, causa pendente o sequestro di documenti); iii) qualora il richiedente di un secondo PEP invochi un interesse nazionale o legittimo.

Concessione del PEP

La decisione di concedere il PEP comune può essere:

- automatica – approvazione automatica mediante il sistema di gestione delle domande SIPEP dopo la convalida dell'identità del richiedente e l'assenza di precedenti penali (tramite riferimenti incrociati con le banche dati dell'anagrafe IRN e dei casellari giudiziari) e di cause pendenti. Ha luogo soltanto nel SEF per le domande di PEP presentate nel continente[78];
- soggetta all'accoglimento/approvazione individuale da parte di altri enti (amministrazioni regionali e consolati) oppure, nel caso del SEF, a requisiti non rientranti nella concessione automatica[79].

[77] Il SIPEP è accessibile (tramite web) a livello nazionale/regionale e internazionale dai servizi situati nel continente, nelle regioni autonome delle Azzorre e di Madera e all'estero (consolati portoghesi).

[78] Si tratta di una funzionalità automatica del sistema di gestione delle domande SIPEP per l'accoglimento (definito internamente "autorizzazione") di una domanda (tranne il caso di un secondo PEP) presentata da un cittadino maggiorenne, provvisto di carta d'identità valida, su cui non incombono cause pendenti o alcun tipo di interdizione. Circa il 60 % dei PEP comuni concessi dal SEF è stato rilasciato con procedure di convalida e decisioni di concessione automatiche, mentre il resto è stato sottoposto all'esame e all'approvazione della *Direção Central de Imigração e Documentação (DCID)*.

[79] In particolare nel caso di richiedenti che non possono esercitare i propri diritti (minori, persone incapaci o soggette a interdizione giudiziale), persone soggette a interdizione legale o a provvedimenti di polizia oppure, nel caso di un secondo PEP, la cui domanda è esaminata individualmente dal DCID.

Rilascio del PEP

Il rilascio del PEP, che comprende produzione, personalizzazione e consegna, è di competenza dell'INCM. Quando la consegna del PEP è registrata nel SIPEP lo stato del passaporto è modificato in "valido".

Le tariffe del PEP variano in funzione del livello di servizio richiesto. Per misurare il livello di servizio il SIPEP deve prendere in considerazione l'effettiva data di consegna del PEP.

La consegna del PEP è effettuata con servizio di corrieri a contratto.

Disattivazione del PEP

Quando un richiedente consegna un PEP precedente ancora valido, questo dev'essere disattivato per impedirne il riutilizzo e lo stato di registrazione del passaporto è cambiato in "inutilizzabile" nel sistema applicativo SIPEP.

Finlandia
Valtiontalouden tarkastusvirasto

Disposizioni di ciberprotezione

Data di pubblicazione: 2017

Link alla relazione: Relazione (versione finlandese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2016-2017

Sintesi della relazione

Tema dell'audit

Lo scopo dell'audit era verificare se la ciberprotezione nell'amministrazione centrale fosse stata predisposta nel modo più efficace ed efficiente possibile in termini di costi. L'audit si è incentrato sull'organizzazione e alla gestione della cibersicurezza da parte dell'amministrazione centrale. Le risultanze dell'audit potrebbero servire a sviluppare l'efficacia e l'efficienza della cibersicurezza nell'amministrazione centrale. L'audit ha avuto luogo dal 22 settembre 2016 al 4 settembre 2017. Nell'autunno 2019 è stato condotto un audit di follow-up. In tale occasione, l'istituzione superiore di controllo ha esaminato le azioni adottate sulla base delle constatazioni e delle raccomandazioni dell'audit.

Sono state sottoposte ad audit le autorità responsabili della ciberprotezione nell'amministrazione centrale (l'ufficio del Primo ministro, il ministero delle Finanze, il ministero dei Trasporti e delle comunicazioni) e le autorità responsabili di compiti di ciberprotezione centralizzata e di servizi informatici centralizzati nell'amministrazione centrale (il centro nazionale di cibersicurezza dell'agenzia finlandese dei trasporti e delle comunicazioni, il centro TIC per l'amministrazione centrale Valtori, l'agenzia dei servizi digitali e dei dati demografici). L'efficacia degli orientamenti è stata valutata altresì esaminando le unità dell'amministrazione centrale che erogano servizi

elettronici (l'agenzia dei servizi digitali e dei dati demografici, l'agenzia finlandese dei trasporti e delle comunicazioni Traficom, l'ufficio amministrativo nazionale per l'applicazione della legge e l'ente da cui dipende, il ministero della Giustizia, nonché il centro servizi TIC del ministero della Giustizia).

Quesiti di audit

Nell'audit sull'organizzazione della cibersicurezza sono stati posti i seguenti quesiti di audit.

- Nell'organizzazione della cibersicurezza l'entità controllata ha accordato sufficiente attenzione all'aspetto economico?
- La consapevolezza situazionale in materia di cibersicurezza dell'entità controllata favorisce la cibersicurezza dei sistemi?
- La capacità dell'entità controllata di rispondere alle violazioni cibernetiche è sufficiente?

Il tema di audit delle disposizioni di ciberprotezione rientrava nel campo di audit "Garantire l'affidabilità operativa della società dell'informazione" compreso nel piano di audit 2016-2020 dell'istituzione superiore di controllo nazionale finlandese. Dal punto di vista dell'importanza per le finanze dell'amministrazione centrale, si può ricondurre il tema di audit agli svantaggi connessi alle interruzioni del servizio e alle violazioni dei dati, nonché agli effetti negativi della carente cibersicurezza sulle attività economiche. L'audit è stato svolto parallelamente all'audit "Guidare l'affidabilità operativa dei servizi elettronici" che si occupa dello stesso argomento. Il principale materiale dell'audit consisteva in documenti e colloqui con le autorità responsabili dell'attività in questione.

Constatazioni e conclusioni

La strategia della Finlandia in materia di cibersicurezza definisce gli obiettivi e le strategie principali per rispondere alle sfide che si pongono all'ambiente informatico e garantirne il funzionamento. Sono stati compiuti sforzi per realizzare la strategia in materia di cibersicurezza tramite un programma di attuazione, i cui progressi sono valutati ogni anno. Il comitato per la sicurezza è un organismo cooperativo in seno al ministero della Difesa che monitora e coordina l'attuazione della strategia per la cibersicurezza.

L’efficace organizzazione della cibersicurezza coincide con la gestione del rischio che, per avere successo, esige disposizioni e strutture gestionali efficaci che integrino la gestione del rischio nelle attività a tutti i livelli dell’organizzazione. Come molti altri paesi, la Finlandia e la sua amministrazione centrale non sono autosufficienti in termini di risorse di ciberprotezione. La legislazione dell’Unione europea è cresciuta nel corso del tempo ed è diventata più vincolante. Nella pubblica amministrazione finlandese la responsabilità della ciberprotezione è decentrata: ogni organismo interno è responsabile della propria cibersicurezza. Nell’amministrazione centrale l’attribuzione delle responsabilità per quanto riguarda la natura, l’ampiezza e il materializzarsi delle possibili violazioni cibernetiche è complessa.

A causa di tale complessità è possibile che la risposta a un’anomalia sia troppo lenta e i ridotti finanziamenti hanno limitato l’attuazione della strategia finlandese per la cibersicurezza. Sulla base delle constatazioni di audit, l’istituzione superiore di controllo nazionale è giunta alle seguenti conclusioni e ha formulato le raccomandazioni seguenti per l’organizzazione della cibersicurezza nell’amministrazione centrale:

La gestione operativa delle violazioni più estese della cibersicurezza non è stata definita

La pianificazione della gestione operativa delle violazioni estese della cibersicurezza e la ripartizione delle relative responsabilità consentirebbero di reagire più rapidamente e di organizzare in maniera più adeguata il coordinamento e l’assegnazione delle risorse per le contromisure. Nell’attuale modello operativo ciascuna agenzia è responsabile della propria ciberprotezione. Le competenze disponibili in materia di ciberprotezione non sono però sufficienti e diventa quindi impossibile predisporre un’adeguata ciberprotezione internamente o tramite esternalizzazione.

Alcuni obiettivi della strategia per la cibersicurezza non sono stati conseguiti

Il programma di attuazione della strategia finlandese per la cibersicurezza ha migliorato la ciberprotezione. Alcuni obiettivi del primo programma di attuazione non sono stati conseguiti, poiché il livello di impegno nelle azioni era disomogeneo e non è stato possibile migliorarlo con criteri centralizzati. Il nuovo programma di attuazione comprendeva soltanto azioni per cui le autorità competenti e altri attori avevano espresso il proprio impegno. Impegno e risorse disponibili sono interdipendenti.

L’adeguatezza delle soluzioni di finanziamento per la ciberprotezione non era chiara

Le differenze nello sviluppo della ciberprotezione dipendevano in parte dalla diversa disponibilità di risorse per lo sviluppo presso le singole organizzazioni. Né la normativa sulla formazione del bilancio dello Stato, né il processo di formazione contemplavano procedure per garantire che venissero assegnati fondi a favore dei più importanti obiettivi della ciberprotezione. Agenzie e istituzioni iscrivevano a bilancio gli stanziamenti per la cibersicurezza come spese operative dell’agenzia o istituzione in questione senza una specificata destinazione. Le misure descritte nella strategia per la cibersicurezza della Finlandia sono state attuate soltanto nella misura consentita dagli stanziamenti.

Le modifiche apportate all’organizzazione delle TIC dovrebbero tener conto anche della ciberprotezione

Le modifiche dell’organizzazione delle TIC nell’amministrazione centrale avevano influito sulle disposizioni di ciberprotezione. Per Valtori è stato difficile sviluppare un sistema di cibersicurezza centralizzato. Sono state rilevate carenze nella valutazione dell’adeguatezza delle procedure pratiche di ciberprotezione e nell’attuazione delle nuove disposizioni.

Occorre migliorare la consapevolezza situazionale delle operazioni di cibersicurezza

Il centro di cibersicurezza curava la consapevolezza situazionale della cibersicurezza in tutto il paese. Al momento dell’audit, non vi era alcun obbligo di segnalare le violazioni di cibersicurezza al centro di cibersicurezza. Imporre alle organizzazioni pubbliche di segnalare le violazioni migliorerebbe la situazione, poiché amplierebbe la portata delle procedure centralizzate di individuazione delle violazioni informatiche.

Sulla base di tali considerazioni, l’istituzione superiore di controllo nazionale raccomanda al ministero delle Finanze di definire e attuare un modello complessivo di gestione operativa nel caso di incidenti di cibersicurezza che colpiscano i servizi TIC dell’amministrazione centrale. Il ministero delle Finanze dovrebbe anche individuare le modalità per affrontare il problema della cibersicurezza dei servizi, finanziandoli lungo tutto il ciclo di vita; dovrebbe inoltre migliorare la consapevolezza situazionale a livello operativo, prescrivendo alle autorità di segnalare le violazioni informatiche al centro di cibersicurezza. È stato raccomandato a Valtori di migliorare l’attuazione, la valutazione e lo sviluppo delle procedure di cibersicurezza e l’individuazione di violazioni informatiche.

L’audit di follow-up ha esaminato le modalità di attuazione delle raccomandazioni formulate durante l’audit. L’istituzione superiore di controllo ha ritenuto che il ministero delle Finanze, in quanto autorità competente per l’attuazione delle raccomandazioni, non abbia adottato misure sufficienti per rispondere alle raccomandazioni formulate. La cibersicurezza è stata però rafforzata in Finlandia tramite misure adottate da autorità diverse dal ministero delle Finanze. Era in corso di realizzazione una modifica della gestione strategica della cibersicurezza, che doveva condurre a un modello fondato sul ruolo del direttore della cibersicurezza. Nella proposta di bilancio per il 2020, il governo ha aumentato gli stanziamenti per le autorità dell’amministrazione centrale che assolvono una funzione chiave nel potenziamento della cibersicurezza. Inoltre, Valtori stava adottando misure conformi alla raccomandazione dell’istituzione superiore di controllo nazionale. In conclusione, l’istituzione superiore di controllo nazionale ha rilevato che l’audit di follow-up era necessario, dal momento che alcune raccomandazioni non erano state attuate, e un audit completamente nuovo nel settore era giustificato dalla costante evoluzione in materia di disposizioni di cibersicurezza e ambiente operativo digitale, dai rischi connessi e dall’importanza della cibersicurezza per le finanze dell’amministrazione centrale e per la società.

Svezia
Riksrevisionen

Sistemi informatici obsoleti: un ostacolo a una digitalizzazione efficace

Data di pubblicazione: 2019

Link alla relazione: Sintesi della relazione (versione inglese)
Relazione (versione svedese)

Tipo e periodo dell'audit

Tipo di audit: Controllo di gestione

Periodo sottoposto ad audit: 2018-2019

Sintesi della relazione

Tema dell'audit

L'obsolescenza dei sistemi informatici critici per l'attività svolta comporta un grave rischio in termini di efficienza perché, in proporzione, le organizzazioni sono costrette a investire risorse più cospicue solo per mantenere il sistema. Vi sono quindi fondati motivi per presumere che i sistemi informatici obsoleti comportino un rischio più elevato di gestione inadeguata dei fondi pubblici. Distolgono inoltre in qualche modo la capacità innovativa di un'agenzia per quanto riguarda lo sviluppo di nuovi sistemi informatici. La presenza di sistemi informatici obsoleti non comporta però solamente rischi per le singole agenzie: i problemi di un'agenzia possono avere gravi conseguenze sulla sua capacità di coordinare le operazioni con un'altra agenzia o con un portatore d'interessi privato. L'obsolescenza dei sistemi informatici comporta rischi anche in termini di sicurezza delle informazioni.

Definizione del principale oggetto dell'audit/Quesiti di audit/Contesto

L'audit si proponeva di esaminare l'incidenza dei sistemi informatici obsoleti nell'amministrazione centrale, per valutare se il governo e le autorità avessero adottato misure adeguate per impedire che tali sistemi diventassero un ostacolo a un'efficace digitalizzazione. I quesiti di audit erano i seguenti.

- Le autorità hanno adottato misure idonee per affrontare i problemi associati a sistemi informatici obsoleti?
- Il governo ha adottato misure idonee per affrontare i problemi associati a sistemi informatici obsoleti?

Constatazioni e conclusioni

- L'audit ha rilevato l'esistenza di sistemi informatici obsoleti in un gran numero di agenzie governative. Inoltre in numerose agenzie erano obsoleti uno o più sistemi informatici critici per l'attività svolta. Per quanto risulta all'istituzione superiore di controllo nazionale svedese, quest'informazione rappresenta una novità poiché in precedenza nessuno conosceva l'entità di questo problema nella pubblica amministrazione centrale. Circa l'80 % delle agenzie ha affermato di aver incontrato difficoltà a mantenere il livello di sicurezza delle informazioni in uno o più sistemi per loro critici. Più di un'autorità su dieci ha risposto che questo problema riguardava tutti i sistemi o la maggioranza di essi.
- Una cospicua percentuale delle agenzie esaminate non adottava l'approccio corretto allo sviluppo e alla gestione del supporto informatico. Queste agenzie non si servivano degli strumenti di sviluppo operativo esistenti per determinare come il supporto informatico potesse meglio contribuire a conseguire gli obiettivi delle operazioni essenziali. Un'ampia percentuale delle agenzie sottoposte ad audit era pertanto priva di una descrizione globale dei collegamenti tra strategie, sistemi e processi operativi. Di conseguenza, avevano difficoltà ad analizzare e comprendere in che modo i cambiamenti incidessero sugli obiettivi dell'organizzazione e, quindi, diventava più arduo definire una situazione futura auspicabile.
- Più di metà delle autorità dichiarava che non esisteva un modello approvato per gestire i loro sistemi informatici e prendere decisioni in merito, dalla fase di sviluppo del sistema al graduale abbandono (quella che di solito si definisce "gestione del ciclo di vita"). Secondo l'istituzione superiore di controllo nazionale

svedese, ciò indicava che la gestione del ciclo di vita non veniva eseguita in maniera strutturata e metodica. Anche l'analisi dei rischi presentava carenze, così come la capacità di disaggregare i costi informatici al livello di dettaglio necessario per un processo decisionale valido.

- Quasi il 60 % delle autorità non disponeva di piani di sviluppo del sistema estesi al ciclo di vita per la gran parte dei propri sistemi, a eccezione di uno o pochi sistemi critici. A causa della mancanza di piani per il ciclo di vita e di altra documentazione di pianificazione presso molte agenzie, unitamente alle carenze della gestione del ciclo di vita effettivamente svolta, non è stato possibile concludere che le agenzie in generale avessero assunto una posizione consapevole ed esplicita nei riguardi dei propri sistemi informatici.

- Secondo la valutazione dell'istituzione superiore di controllo nazionale svedese, i ministeri coinvolti, e quindi anche il governo, non avevano una conoscenza sufficiente dell'incidenza e delle conseguenze dell'obsolescenza dei sistemi informatici.

La conclusione generale è stata che, al momento dell'audit, gran parte delle agenzie non era riuscita a gestire in maniera veramente efficace i problemi derivanti dall'obsolescenza dei sistemi informatici. L'ISC nazionale svedese ha giudicato il problema così grave e diffuso da ostacolare una costante ed efficiente digitalizzazione dell'amministrazione statale. L'audit ha altresì dimostrato che il governo non conosceva né l'esistenza né le conseguenze dei problemi legati all'obsolescenza dei sistemi informatici e non aveva adottato alcuna misura per affrontare più direttamente il problema dei sistemi informatici obsoleti. Secondo la valutazione dell'ISC nazionale svedese, pertanto, non si poteva affermare che il governo avesse adottato misure sufficienti per attenuare o risolvere i problemi.

Altre relazioni in questo settore

Titolo della relazione:	Agevolare l'avvio di un'impresa: l'operato del governo per promuovere un processo digitale (RiR 2019:14)
Link alla relazione:	Sintesi della relazione (versione inglese) Relazione (versione svedese)
Data di pubblicazione:	2019
Titolo della relazione:	La digitalizzazione della pubblica amministrazione: un'amministrazione più semplice, più trasparente ed efficace (RiR 2016:14)
Link alla relazione:	Sintesi della relazione (versione inglese) Relazione (versione svedese)
Data di pubblicazione:	2016
Titolo della relazione:	La sicurezza delle informazioni presso nove agenzie (RiR 2016:8)
Link alla relazione:	Sintesi della relazione (versione inglese) Relazione (versione svedese)
Data di pubblicazione:	2016
Titolo della relazione:	Cibercriminalità: polizia e pubblici ministeri possono essere più efficienti (RiR 2015:21)
Link alla relazione:	Sintesi della relazione (versione inglese) Relazione (versione svedese)
Data di pubblicazione:	2015

Unione europea
Corte dei conti europea

Documento di riflessione: Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza

Data di pubblicazione: 2018

Link alla relazione: Relazione (23 versioni linguistiche)

Tipo e periodo dell'audit

Tipo di audit: Analisi delle politiche

Periodo sottoposto ad audit: Aprile - settembre 2018

Sintesi della relazione

Tema dell'analisi

Questo documento di riflessione, che non costituisce una relazione di audit, intende offrire una panoramica dell'articolata politica dell'UE in materia di cibersicurezza e individuare le principali sfide per una sua efficace realizzazione. Affronta i temi della sicurezza delle reti e dell'informazione, della criminalità informatica, della ciberdifesa e della disinformazione.

L'analisi della Corte era basata su un esame documentale di informazioni pubblicamente disponibili in documenti ufficiali, documenti di sintesi e studi di terzi. L'attività sul campo è stata svolta tra aprile e settembre 2018 e teneva conto degli sviluppi fino al dicembre 2018. Tale lavoro è stato integrato da un'indagine presso le istituzioni superiori di controllo degli Stati membri e da colloqui intrattenuti con importanti portatori di interesse delle istituzioni dell'UE e con rappresentanti del settore privato.

Non esiste una definizione convenzionale di cibersicurezza. In termini ampi, essa designa il complesso di tutele e misure adottate per difendere i sistemi informativi e i relativi utenti da accessi non autorizzati, attacchi e danni al fine di assicurare la riservatezza, l'integrità e la disponibilità dei dati. Nella cibersicurezza rientrano la prevenzione e l'individuazione degli incidenti informatici, la risposta agli stessi e il

successivo recupero. Gli incidenti possono essere intenzionali o meno e vanno, ad esempio, dalla divulgazione accidentale di informazioni agli attacchi a imprese e infrastrutture critiche, dal furto di dati personali fino addirittura all'interferenza nei processi democratici.

L'approccio strategico dell'UE ruota attorno alla strategia per la cibersicurezza del 2013. Questa intende rendere l'ambiente digitale dell'UE il più sicuro al mondo, difendendo al contempo i valori e le libertà fondamentali. Si pone cinque obiettivi principali: i) accrescere la ciber-resilienza; ii) ridurre la criminalità informatica; iii) sviluppare politiche e capacità di ciberdifesa; iv) sviluppare le risorse industriali e tecnologiche per la cibersicurezza; v) creare una politica internazionale relativa al ciberspazio che sia in linea con i valori fondanti dell'UE.

Constatazioni

In mancanza di dati attendibili, non era facile cogliere l'impatto di una insufficiente preparazione a un attacco informatico. L'impatto economico della criminalità informatica si è quintuplicato tra il 2013 e il 2017, colpendo amministrazioni pubbliche e imprese, grandi e piccole indifferentemente. A fronte di questa tendenza, si prevede un aumento dei premi di assicurazione informatica dai 3 miliardi di euro del 2018 a 8,9 miliardi di euro nel 2020. Benché l'80 % delle imprese dell'UE abbia subito almeno un incidente di cibersicurezza nel 2016, i rischi al riguardo sono ancora ignorati in misura allarmante. Tra le imprese nell'UE, il 69 % ha una comprensione nulla o solo basilare della propria esposizione alle ciberminacce e il 60 % non ha mai stimato le potenziali perdite finanziarie. Stando a un sondaggio mondiale, un terzo delle organizzazioni preferirebbe pagare il riscatto chiesto dagli hacker che investire nella sicurezza delle informazioni.

La Corte ha formulato le seguenti constatazioni:

- l'ecosistema cibernetico dell'UE è complesso e stratificato e coinvolge molti portatori d'interessi. Fare di tutte le sue disparate parti un complesso organico è una sfida non da poco;

- l'UE aspira a creare l'ambiente online più sicuro al mondo. Per realizzare questa ambizione, tutte le parti in causa devono compiere sforzi significativi, tra cui anche assicurare un solido fondamento finanziario accuratamente gestito. Per quanto difficile da quantificare, la spesa del settore pubblico dell'UE per la cibersicurezza si collocherebbe, secondo le stime, tra uno e due miliardi di euro

all'anno. A titolo di confronto, le spese iscritte a bilancio dal governo federale degli Stati Uniti nel 2019 ammontavano a circa 21 miliardi di dollari;

- la governance della sicurezza delle informazioni consiste nel porre in atto strutture e politiche che assicurino la riservatezza, l'integrità e la disponibilità dei dati. Non si tratta solo di una questione tecnica; sono necessari una leadership efficace, processi solidi e strategie allineate con gli obiettivi organizzativi;

- i modelli di governance della cibersicurezza differiscono da uno Stato membro all'altro e, nell'ambito di detti modelli, la responsabilità per la cibersicurezza è spesso suddivisa tra molte entità. Queste differenze potrebbero ostacolare la collaborazione necessaria per rispondere ad incidenti transfrontalieri su vasta scala nonché per scambiare intelligence sulle minacce a livello nazionale e, ancor più, a livello dell'UE;

- ideare una risposta efficace ai ciberattacchi è cruciale per bloccarli il prima possibile. È particolarmente importante che i settori critici, gli Stati membri e le istituzioni dell'UE siano in grado di rispondere in modo celere e coordinato. A tale scopo è essenziale una rapida individuazione.

Raccomandazioni

Dall'analisi svolta dalla Corte risulta che è necessario passare ad una cultura della performance, che integri pratiche di valutazione, per assicurare una rendicontabilità e una valutazione che abbiano senso. Permangono alcune lacune nella normativa e le norme esistenti non sono recepite in modo uniforme dagli Stati membri. Ciò può rendere difficile il dispiegamento del pieno potenziale della normativa.

Un'altra problematica individuata concerne l'allineamento tra i livelli di investimento e gli obiettivi strategici: è necessario incrementare i livelli d'investimento e l'impatto degli stessi. Ciò risulta più arduo quando l'UE e i suoi Stati membri non dispongono di una chiara visione d'insieme della spesa dell'UE destinata alla cibersicurezza. Sono stati segnalati anche indizi di scarsa adeguatezza delle risorse assegnate alle agenzie dell'UE operanti nei settori inerenti alla cibersicurezza; dette agenzie hanno anche difficoltà ad attrarre e trattenere persone di talento.

Acronimi e abbreviazioni

AED: Agenzia europea per la difesa

APT: minaccia persistente avanzata

CERS: Comitato europeo per il rischio sistemico

CERT-UE: squadra di pronto intervento informatico

COBIT: obiettivi di controllo nel campo dell'informazione e delle tecnologie correlate

Corte: Corte dei conti europea

COVID-19: malattia da coronavirus 2019

cPPP: partenariato pubblico-privato contrattuale

CSIRT: gruppo di intervento per la sicurezza informatica in caso di incidente

DDoS: attacco distribuito di negazione del servizio

Direttiva NIS: direttiva sulla sicurezza delle reti e dei sistemi informativi

EC3: Centro europeo per la lotta alla criminalità informatica (presso Europol)

ENISA: Agenzia dell'Unione europea per la cibersicurezza

Europol: Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto

Fondi SIE: Fondi strutturali e d'investimento europei

GDPR: regolamento generale sulla protezione dei dati

IoT: Internet delle cose

ISACA: Associazione per il controllo e l'audit dei sistemi informatici

ISC: istituzione superiore di controllo

ISF-P: Fondo sicurezza interna – Polizia

IT: tecnologie dell'informazione

MCE: meccanismo per collegare l'Europa

MERS: sindrome respiratoria del Medio Oriente

NATO: Organizzazione del Trattato del Nord Atlantico

PED: programma Europa digitale

PESCO: quadro di cooperazione strutturata permanente

PIL: prodotto interno lordo

PSDC: politica di sicurezza e di difesa comune

QFP: quadro finanziario pluriennale

RDP: protocollo desktop remoto

SARS: sindrome acuta respiratoria severa

SEAE: servizio europeo per l'azione esterna

TIC: tecnologie dell'informazione e della comunicazione

UE: Unione europea

URL: Uniform Resource Locator (identificatore uniforme di risorse)

USA: Stati Uniti d'America

Glossario

5G: standard tecnologico di quinta generazione per le reti cellulari a banda larga, che le imprese di telefonia cellulare hanno iniziato a impiegare in tutto il mondo nel 2019 e che, secondo le previsioni, dovrebbe succedere alle reti 4G che attualmente forniscono la connettività a moltissimi cellulari attuali. L'incremento di velocità si ottiene in parte utilizzando onde radio a frequenza più alta rispetto alle reti cellulari precedenti.

Adware: malware che mostra banner pubblicitari o finestre pop-up che includono linee di codice per tracciare il comportamento online delle vittime.

Attacchi via Internet: utenti specifici confidano nel fatto che le informazioni personali sensibili da essi divulgate sul sito web rimangano private e sicure. Un'intrusione (attacco) può far sì che informazioni mediche oppure i dati relativi alla carta di credito o alla previdenza sociale diventino pubblici, con conseguenze potenzialmente gravi.

Attacco distribuito di negazione del servizio (DDoS): ciberattacco che impedisce agli utenti che ne hanno titolo di accedere ad un servizio o ad una risorsa online, inondando quest'ultimo o quest'ultima con un numero di richieste superiore a quelle che può gestire.

Bene digitale: qualunque cosa esista in formato digitale, di proprietà di un privato o di un'impresa, e sia associata al diritto di utilizzo (ad esempio immagini, foto, video, file contenenti testo, ecc.).

Bitcoin: valuta digitale o virtuale creata nel 2009 che utilizza una tecnologia peer-to-peer per favorire i pagamenti istantanei.

Calcolo ad alte prestazioni: capacità di trattare dati ed eseguire calcoli complessi ad alta velocità.

Ciberattacco o attacco informatico: atto deliberato mirante a compromettere o distruggere la riservatezza, l'integrità e la disponibilità dei dati o di un sistema computerizzato attraverso il ciberspazio.

Cibercriminalità o criminalità informatica: varie attività criminali che coinvolgono computer e sistemi informatici, come strumento o come bersaglio primario. Fra dette attività figurano: reati tradizionali (ad esempio frode, falsificazione e furto di identità); reati connessi ai contenuti (ad esempio distribuzione online di materiale pedopornografico o incitamento all'odio razziale); reati propri ai sistemi computerizzati e informativi (ad esempio attacchi contro sistemi informativi, attacchi mirati alla negazione del servizio, malware o ransomware).

Ciberdifesa: sottoinsieme della cibersicurezza che mira a difendere il ciberspazio tramite mezzi militari ed altri mezzi idonei, al fine di conseguire obiettivi strategico-militari.

Ciberdiplomazia: uso di risorse diplomatiche ed esercizio di funzioni diplomatiche per tutelare gli interessi nazionali in relazione al ciberspazio. Si svolge in tutto o in parte grazie all'azione dei diplomatici, che si riuniscono in incontri bilaterali (come avviene per il dialogo Stati Uniti-Cina) o in consessi multilaterali (come nel caso delle Nazioni Unite). Oltre al tradizionale ambito della diplomazia, essi interagiscono anche con vari attori non statali, come i dirigenti delle imprese di Internet (ad esempio Facebook o Google), gli imprenditori del settore tecnologico oppure le organizzazioni della società civile. Grazie alla tecnologia, la diplomazia può anche dare voce agli oppressi di altri paesi.

Ciberincidente o incidente di cibersicurezza: evento che danneggia o minaccia, direttamente o indirettamente, la resilienza e la sicurezza di un sistema informatico e dei dati da questo trattati, immagazzinati o trasmessi.

Ciberminaccia: atto doloso teso a danneggiare o rubare dati, oppure a perturbare la vita digitale in generale.

Ciber-resilienza: capacità di prevenire, prepararsi a, sopportare e riprendersi a seguito di ciberattacchi o ciberincidenti.

Cibersicurezza (ciberprotezione): il complesso di tutele e misure adottate per difendere i sistemi informatici e i relativi dati da accessi non autorizzati, attacchi e danni, al fine di assicurarne la riservatezza, l'integrità e la disponibilità.

Ciberspazio: ambiente mondiale immateriale nel quale si verificano le comunicazioni online tra persone, software e servizi tramite reti di computer e dispositivi tecnologici.

Ciberspionaggio: atto o pratica che consiste nell'ottenere, tramite Internet, reti o singoli computer, segreti e informazioni da privati cittadini, concorrenti, rivali, gruppi, governi e nemici, senza il permesso di chi li detiene o senza che questi ne sia a conoscenza, per trarne un vantaggio personale, economico, politico o militare.

Cifratura: trasformazione di informazioni leggibili in un codice illeggibile, al fine di proteggerle. Per poter leggere le informazioni, l'utente deve avere accesso ad una chiave o a una password segreta.

Contenuto digitale: qualunque dato (costituito da testi, suoni, immagini o video) conservato in formato digitale.

Criptovaluta: bene digitale emesso e scambiato usando tecniche di cifratura, in modo indipendente da una banca centrale. Viene accettato come mezzo di pagamento dai membri di una comunità virtuale.

Dati biometrici (biometria): calcoli fisici (impronte digitali e iride) o comportamentali connessi alle caratteristiche umane. L'autenticazione è utilizzata in informatica come una forma di identificazione e controllo dell'accesso.

Dati di accesso: informazioni sull'attività di autenticazione (log in) e di disconnessione (log out) che un utente svolge per accedere ad un servizio; tali informazioni comprendono l'orario, la data e l'indirizzo IP.

Dati personali: informazioni relative a una persona fisica identificabile.

Digitalizzazione: processo di conversione delle informazioni in un formato digitale, durante il quale le informazioni sono organizzate in bit. Il risultato consiste nella rappresentazione di un oggetto, un'immagine, un suono, un documento o un segnale mediante la generazione di una serie di numeri che descrivono una serie discreta di punti o campioni.

Disinformazione: informazioni che è possibile dimostrare come false o fuorvianti; sono concepite, presentate e diffuse a scopo di lucro o per ingannare intenzionalmente il pubblico e possono arrecare un pregiudizio pubblico.

Disponibilità: garanzia di accesso tempestivo e attendibile alle informazioni e relativo impiego.

Ecosistema cibernetico: insieme complesso di dispositivi, dati, reti, persone, processi ed organizzazioni che interagiscono fra loro, insieme all'ambiente dei processi e delle tecnologie che influenzano e sostengono dette interazioni.

Fornitore di servizio digitale: chiunque fornisca uno o più dei seguenti tre tipi di servizi digitali: mercato online, motore di ricerca online e servizi di cloud computing.

Hacker etico: individuo (esperto di sicurezza informatica) che penetra in una rete informatica per testarne o valutarne la sicurezza e non per perseguire finalità dolose o criminali.

Hacker: individuo che si avvale di computer, attività di rete o altre competenze per accedere senza autorizzazione a dati, reti o sistemi informatici.

Impianti dei servizi di pubblica utilità: qualunque palo, torre, conduttura aerea o sotterranea, o qualsiasi altra struttura di sostegno o supporto oppure di canalizzazione, accessori compresi, utilizzabile per la fornitura o la distribuzione di servizi elettrici, telefonici, telegrafici, trasmissioni via cavo o di segnalazione, o di qualsiasi altro servizio analogo.

Infrastruttura critica: risorse fisiche, servizi e strutture il cui danneggiamento o la cui distruzione avrebbe un impatto grave sul funzionamento dell'economia e della società.

Infrastruttura elettorale: infrastruttura che comprende i sistemi informatici e le banche dati per le campagne, le informazioni sensibili sui candidati, la registrazione degli elettori e i sistemi di gestione.

Ingegneria sociale: nella sicurezza delle informazioni, manipolazione psicologica per indurre con l'inganno le vittime a compiere un'azione o a divulgare informazioni riservate.

Installazione di patch: introduzione di un insieme di modifiche al software, al fine di aggiornarlo, di correggere errori, di migliorarlo; comprende l'eliminazione di vulnerabilità relative alla sicurezza.

Integrità: tutela dalla modifica impropria delle informazioni o dalla loro distruzione, a garanzia della loro autenticità.

Intelligenza artificiale: la simulazione dell'intelligenza umana con macchine programmate per pensare come esseri umani e riprodurne le azioni; qualsiasi macchina con caratteristiche associate alla mente umana, come l'apprendimento e la soluzione di problemi.

Internet delle cose (Internet of Things, IoT): rete di oggetti d'uso quotidiano dotati di sistemi elettronici, software e sensori in modo da poter comunicare e scambiare dati via Internet.

Malware: software scritto con finalità dolose; programma informatico concepito per danneggiare un computer, un server o una rete.

Minaccia ibrida: atto ostile compiuto da avversari mediante il ricorso a una combinazione di tecniche di guerra convenzionali e non convenzionali (ossia mezzi militari, politici, economici e tecnologici) nell'accanito perseguimento dei loro obiettivi.

Minaccia persistente avanzata: un attacco in cui un utente non autorizzato ottiene l'accesso a un sistema o a una rete e vi rimane per un lungo periodo senza essere individuato. È particolarmente pericoloso per le imprese, dal momento che i pirati informatici hanno costante accesso a dati sensibili dell'azienda; di solito però non danneggia le reti dell'azienda né i computer locali. L'obiettivo è il furto di dati.

Nuvola informatica (cloud computing): prestazione su richiesta di risorse informatiche (quali archiviazione, potenza di calcolo o capacità di condivisione dei dati) attraverso Internet, tramite hosting su server remoti.

Operatore di servizi essenziali: ente pubblico o privato che fornisce un servizio essenziale per il mantenimento di attività sociali ed economiche fondamentali.

Phishing: pratica consistente nell'inviare messaggi di posta elettronica, all'apparenza provenienti da un mittente fidato, allo scopo di indurre con l'inganno i destinatari a cliccare su link che diffondono malware o a condividere informazioni personali.

Piattaforma digitale: ambiente che consente interazioni tra almeno due gruppi differenti: di solito uno è costituito dai fornitori e l'altro dai consumatori/utenti. Può trattarsi dell'hardware o del sistema operativo, di un browser e delle interfacce di programmazione delle applicazioni (application programming interface, API) associate, o ancora di un altro software sottostante, purché il codice di programma sia eseguito con esso.

Protocollo di desktop remoto (RDP): standard tecnico (elaborato da Microsoft) per utilizzare un computer da tavolo a distanza. Gli utenti del desktop remoto possono accedere al proprio desktop, aprire e modificare file e utilizzare applicazioni esattamente come se fossero di fronte al proprio computer.

Ransomware: malware che impedisce l'accesso delle vittime a un sistema informatico o che rende illeggibili i file, in genere mediante cifratura. Di solito, l'autore dell'attacco ricatta in seguito la vittima, chiedendo il pagamento di un riscatto per ripristinare l'accesso.

Riservatezza: protezione delle informazioni, dei dati o dei beni da accessi o divulgazione non autorizzati.

Sabotaggio: azione deliberata tesa a distruggere, recare danno o creare ostacoli, soprattutto per trarne vantaggi politici o militari.

Sicurezza della rete: sottoinsieme della cibersicurezza che protegge i dati inviati tramite dispositivi sulla stessa rete, per impedire che le informazioni vengano intercettate o modificate.

Sicurezza delle informazioni: insieme di processi e strumenti che tutelano i dati fisici e digitali da un accesso, utilizzo, divulgazione, interruzione, modifica, registrazione o distruzione non autorizzati.

Sistema informativo essenziale: qualsiasi sistema informativo, esistente o previsto, che sia considerato essenziale per il funzionamento efficiente ed efficace dell'organizzazione.

Spyware: software malevolo che mira a raccogliere informazioni su una persona o un'organizzazione e a inviare tali informazioni a un'altra entità in modo da danneggiare l'utente, per esempio violando la riservatezza dei suoi dati personali o mettendo a repentaglio la sicurezza del dispositivo.

Trattamento dei dati: esecuzione di operazioni sui dati, in particolare tramite un computer, per recuperare, trasformare o classificare le informazioni.

Trojan: tipo di codice o software malevolo che, pur sembrando legittimo, può assumere il controllo del computer. Un Trojan è concepito per danneggiare, causare interruzioni, perpetrare furti o in generale produrre altri effetti dannosi sui dati o sulle reti.

Vettorizzazione del testo: conversione di parole, frasi o interi documenti in vettori numerici che possono essere utilizzati da algoritmi di apprendimento automatico (machine-learning).

Violazione dei dati: divulgazione intenzionale o accidentale di informazioni protette o private/riservate in un ambiente non affidabile.

Worm: programma di malware a sé stante, che si replica per diffondersi su altri computer; è detto anche "worm informatico". Utilizza spesso una rete informatica per diffondersi, sfruttando le falle nella sicurezza del computer bersaglio per accedervi.

Per contattare l'UE

Di persona
I centri di informazione Europe Direct sono centinaia, disseminati in tutta l'Unione europea. Potete trovare l'indirizzo del centro più vicino sul sito https://europa.eu/european-union/contact_it

Telefonicamente o per email
Europe Direct è un servizio che risponde alle vostre domande sull'Unione europea. Il servizio è contattabile:
— al numero verde: 00 800 6 7 8 9 10 11 (presso alcuni operatori queste chiamate possono essere a pagamento),
— al numero +32 22999696, oppure
— per e-mail dal sito https://europa.eu/european-union/contact_it

Per informarsi sull'UE

Online
Il portale Europa contiene informazioni sull'Unione europea in tutte le lingue ufficiali:
https://europa.eu/european-union/index_it

Pubblicazioni dell'UE
È possibile scaricare o ordinare pubblicazioni dell'UE gratuite e a pagamento dal sito https://publications.europa.eu/it/publications. Le pubblicazioni gratuite possono essere richieste in più esemplari contattando Europe Direct o un centro di informazione locale (cfr. https://europa.eu/european-union/contact_it).

Legislazione dell'UE e documenti correlati
La banca dati Eur-Lex contiene la totalità della legislazione UE dal 1952 in poi in tutte le versioni linguistiche ufficiali:
https://eur-lex.europa.eu

Open Data dell'UE
Il portale Open Data dell'Unione europea (http://data.europa.eu/euodp/it) dà accesso a un'ampia serie di dati prodotti dall'Unione europea. I dati possono essere liberamente utilizzati e riutilizzati per fini commerciali e non commerciali.

Contact Committee

Comitato di contatto

delle Istituzioni superiori di controllo dell'UE