enisa

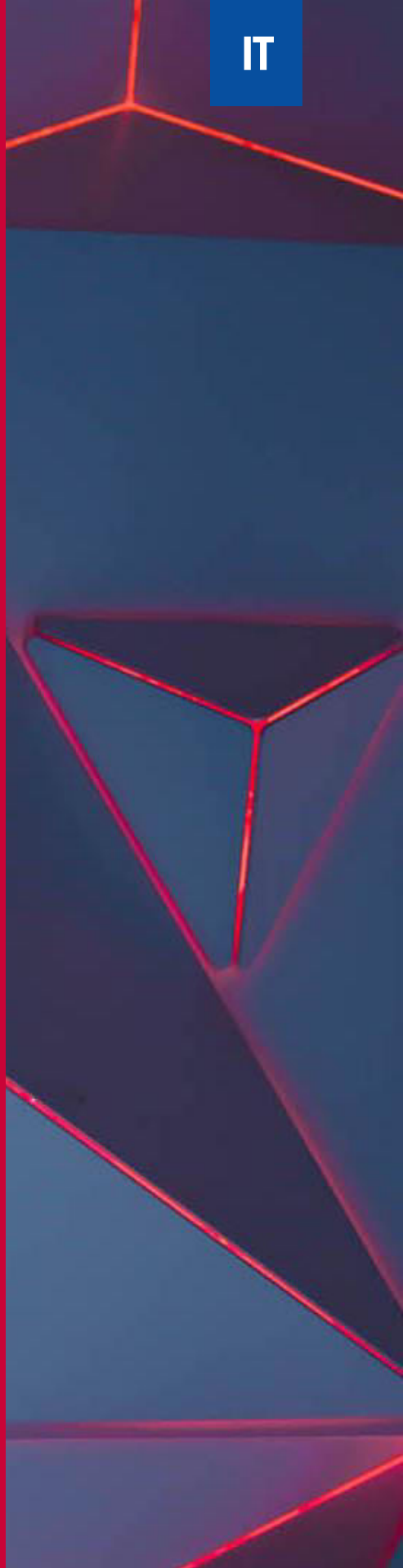
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Manipolazione/danno/furto/perdita di natura fisica

Panorama delle minacce analizzato dall'ENISA



Quadro generale

La manomissione, il danneggiamento, il furto e la perdita di natura fisica sono cambiati drasticamente negli ultimi anni. L'integrità dei dispositivi è vitale perché la tecnologia diventi mobile e per la maggior parte delle implementazioni dell'Internet degli oggetti (IoT). L'IoT può migliorare la sicurezza fisica con soluzioni più avanzate e complesse.[1] In questo modo, i sistemi basati sulla sicurezza IP con sensori intelligenti, telecamere Wi-Fi, illuminazione di sicurezza intelligente, droni e serrature elettroniche possono fornire dati di sorveglianza, valutabili da meccanismi di intelligenza artificiale (IA) e apprendimento automatico (Machine Learning, ML) per identificare le minacce e rispondere con il minimo ritardo e la massima precisione.[2] Tuttavia, gli edifici intelligenti, i dispositivi mobili e i dispositivi indossabili intelligenti possono essere sfruttati per aggirare le misure di sicurezza fisica.[3]

Nel 2019 gli attacchi fisici correlati a sportelli automatici e terminali POS sono continuati in Europa e nel mondo, ma le perdite risultanti sono state inferiori alla media dell'ultimo decennio. La buona notizia è che aziende, responsabili IT e decisori si stanno orientando verso piani di sicurezza ciberfisica ibridi, anche se in passato la sicurezza fisica non rappresentava una priorità.

_Pratiche di sicurezza nuove e obsolete

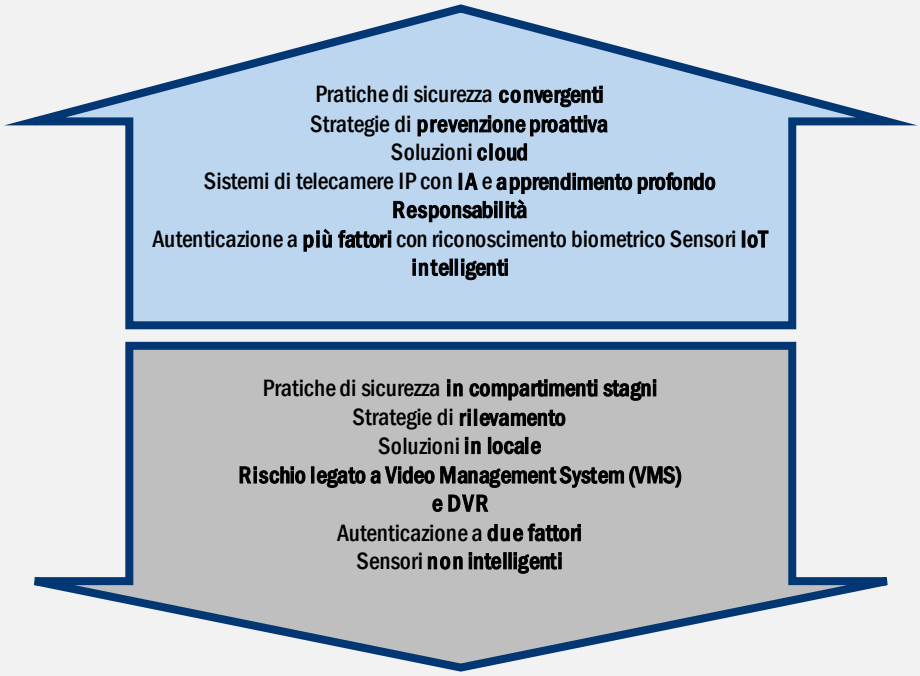


Figura 1 - Fonte: Boonedam blog[4]

Kill chain

Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo

Danno/perdita/furto di natura fisica

Installazione

Command & Control (Comando e controllo)

Actions on Objectives (Azioni sugli obiettivi)

Il modello Cyber Kill Chain® è stato sviluppato da Lockheed Martin, che lo ha adattato da un concetto militare legato alla struttura di un attacco. Per studiare un particolare vettore di attacco, si può utilizzare questo modello per mappare ogni fase del processo e fare riferimento agli strumenti, alle tecniche e alle procedure impiegate dall'aggressore.

MAGGIORI INFORMAZIONI

Tenden

L'accesso fisico è la maggiore backdoor

Nell'aprile 2019 Vishwanath Akuthota si è dichiarato colpevole di vandalismo, per la distruzione di apparecchiature con una scarica elettrica utilizzando un dispositivo USB malevolo. I dispositivi distrutti erano di proprietà del College of Saint Rose di Albany, New York, università in cui Akuthota si era laureato. Ai fini dell'attacco, ha avuto accesso a 66 postazioni di lavoro e a numerosi monitor e podi digitali. La chiavetta «USB killer» da lui utilizzata è stata acquistata online. Il college ha speso più di 50 000 dollari USA (circa 42 452 euro) per sostituire l'attrezzatura e più di 7 000 dollari (circa 5 943 euro) per retribuire il dipendente che si è occupato dell'incidente. Akuthota si è trovato di fronte a una pena di 10 anni di reclusione e una multa massima di 250 000 dollari USA (circa 212 257 euro).[5]

Scarsa attenzione delle aziende alla sicurezza fisica

Nel corso del 2019 sono state effettuate diverse indagini sulla sicurezza fisica, alcune delle quali incentrate su amministratori delegati, responsabili IT e decisori di diversi settori. I risultati forniscono un quadro chiaro del modo in cui viene gestita la sicurezza fisica all'interno delle aziende. Gli amministratori delegati di vari settori industriali sembrano propendere per un piano combinato di sicurezza ciberfisica per proteggere gli asset dalle minacce, considerando fattori quali le minacce interne, l'importanza dell'infrastruttura e l'integrità delle reti aziendali. In questi piani di sicurezza combinati, la maggior parte dell'attenzione, del budget e del personale è stata dedicata agli investimenti nella cibersicurezza (vale a dire l'83-86% delle rispettive risorse), mentre il 14-17% delle risorse aziendali è stato destinato alla sicurezza fisica. In Europa la maggior parte dei responsabili IT (77%) ha dichiarato che la sicurezza fisica dei beni della propria azienda era obsoleta.[7]

_Sicurezza fisica in modalità «as-a-service»

Una tendenza osservata nel 2019 è stata quella di migliorare la sicurezza fisica attivando soluzioni di sicurezza in hosting. Nei rispettivi piani di sicurezza, la maggior parte dei responsabili IT si era già orientata verso schemi basati su cloud e IoT o prevedeva di farlo entro 12 mesi. Secondo quanto riferito dai decisori, erano già in fase di valutazione soluzioni di videosorveglianza «as-a-service» (VSaaS) e di controllo degli accessi «as-a-service» (ACaaS) per migliorare il rilevamento degli incidenti e i tempi di risposta e ridurre le percentuali di falsi positivi. Le soluzioni VSaaS e ACaaS hanno potenziato sia la sicurezza fisica sia la sicurezza informatica, sebbene solo alcuni dei responsabili IT abbiano citato la sicurezza fisica come priorità.[8]

_La sicurezza fisica degli sportelli automatici non ha retto alla prova del tempo

Come già osservato nel 2018, nel periodo in esame gli sportelli automatici si sono rivelati vulnerabili alle manomissioni e al danneggiamento fisico finalizzati al furto del denaro all'interno. In Irlanda, solo nel primo trimestre del 2019 sono stati segnalati nove incidenti.[9] Alcuni degli attacchi sono stati clamorosi, con l'uso di escavatori rubati, l'abbattimento di muri e lo sdradicamento degli sportelli con successivo trasporto degli stessi in furgoni o automobili. In altri casi gli attacchi sono stati portati a termine in pochi minuti con l'uso di esplosivi, catene e sfondamento.[10] Nei Paesi Bassi, in un solo fine settimana di novembre sono stati compiuti 71 attacchi con esplosivo a sportelli automatici (Plofkraken in olandese), rispetto a 43 attacchi simili nel corso dell'intero 2018. La banca ABN AMRO è stata costretta a rimuovere 470 sportelli automatici vulnerabili e l'associazione bancaria olandese (NVB) ha deciso di chiudere tutti gli sportelli automatici a livello nazionale ogni notte tra le 23.00 e le 7.00 nel mese di dicembre.[11] Il 2019 è il quarto anno consecutivo in cui si registra un aumento degli attacchi fisici agli sportelli automatici.

Tendenze

Manomissione degli sportelli automatici

Nel corso del 2019 le principali espressioni di manomissione degli ATM sono state la cattura delle carte (card trapping), la cattura delle banconote (cash trapping) e la frode legata all'annullamento dell'operazione di prelievo (transaction reversal fraud). Nel quadro generale dell'anno si osserva una diminuzione delle manomissioni di sportelli automatici e pompe di benzina, grazie all'aumento dei pagamenti EMV. Lo standard EMV, che prende il nome dalle tre società che lo hanno introdotto (Europay, Mastercard e Visa), descrive le specifiche per le smart card, i terminali di pagamento e gli sportelli automatici. Le carte EMV (note anche come chip e PIN o carte con chip) contengono circuiti integrati. L'adozione delle carte EMV ha interrotto, almeno in parte, le frodi con presenza fisica delle carta.[12] Purtroppo le carte EMV non sono ampiamente diffuse al di fuori dell'Europa e, anche in territorio europeo, solo pochi paesi hanno adottato il sistema Geocontrol, un programma antifrode delle carte EMV.[13]

Incidenti

- La violazione compiuta con chiavetta USB Killer evidenzia la necessità di sicurezza fisica. Vishwanath Akuthota, ex allievo del College of Saint Rose di Albany, New York, si è dichiarato colpevole di avere vandalizzato apparecchiature mediante un dispositivo USB malevolo.[5]
- I malviventi si servono di escavatori per rubare gli sportelli automatici in Irlanda del Nord. Il numero di attacchi fisici agli sportelli automatici è in aumento in tutta l'UE.[9]
- Plofkraken olandesi. Attacchi con esplosivo (noti come «Plofkraken») ai danni degli sportelli automatici olandesi, per lo più concentrati su quelli della banca ABN AMRO a causa di una vulnerabilità. Hanno indotto la banca a rimuovere circa 470 dei suoi sportelli automatici in tutti i Paesi Bassi.[11]

Risultati

Il 4% delle violazioni è stato causato da azioni fisiche[12]

Il 20% degli incidenti di cibersicurezza è iniziato o si è concluso con un'azione fisica[12]

Al 5° posto tra le azioni dolose più frequenti a danno di asset vi sono gli attacchi fisici agli sportelli automatici[12]

Il 54% delle violazioni dei dati in tutti i settori includeva un attacco fisico come metodo principale

Il 48% dei responsabili IT utilizza videosorveglianza o controllo degli accessi basati su cloud[8]

Il 72% dei dipendenti ritiene che lasciare informazioni sensibili in aree accessibili al pubblico rappresenti la minaccia più grave per la sicurezza dei dati[14]

Il 65% degli oltre 1 000 dipendenti intervistati ha riferito di avere tenuto comportamenti e adottato pratiche identificati come rischiosi per la sicurezza fisica[15]

Mitigazione

Azioni proposte

- Utilizzare la crittografia nell'archiviazione e nel flusso di tutte le informazioni che si trovano al di fuori del perimetro di sicurezza (dispositivi, reti, servizi cloud, ecc.).
- Utilizzare inventari degli asset per tenere traccia dei dispositivi degli utenti e ricordare ai proprietari di verificare la disponibilità.
- Assicurare l'accesso limitato alle aree contenenti informazioni o apparecchiature sensibili.
- Attuare politiche di sicurezza fisica ben documentate e integrare le misure di sicurezza fisica con quelle digitali, per realizzare un approccio olistico.
- Utilizzare polizze di assicurazione a copertura dei danni per i rischi sia fisici che informatici.
- Elaborare guide per l'utente per i dispositivi mobili (smartphone, tablet, laptop, ecc.) e seguire le migliori pratiche.
- Stabilire procedure correttamente comunicate per la protezione fisica degli asset, tra l'altro da perdita, danneggiamento e furto.
- Garantire che i dispositivi siano smaltiti solo dopo che siano state cancellate dagli stessi informazioni personali o sensibili in modo sicuro.[6]
- Ridurre i tempi di risposta per gli eventi di furto, danneggiamento e smarrimento.
- Implementare un'autenticazione a più fattori, che combini le credenziali utente con il riconoscimento biometrico, le smart card o altri token fisici.[16]
- Ispezionare periodicamente i dispositivi per rilevare eventuali alterazioni o sostituzioni.[6]
- Adottare processi per il rilevamento dei visitatori o dipendenti autorizzati e assegnare diritti di accesso appropriati.[6]
- Installare sistemi di monitoraggio degli accessi, sistemi di controllo degli accessi, credenziali di accesso forti e dispositivi di accesso intelligenti (ad esempio serrature intelligenti, chiavi intelligenti) per le aree che ospitano apparecchiature sensibili.[6]

_Alternative preferibili per le credenziali dell'utente nell'autenticazione a più fattori

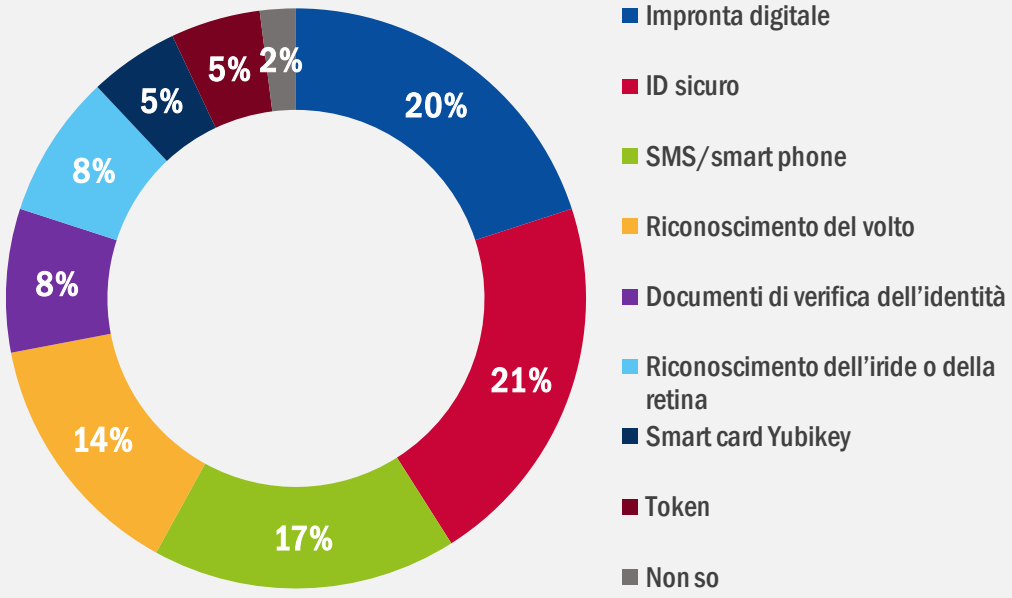


Figura 2 - Fonte: ORACLE & KPMG[16]

Riferimenti bibliografici

1. «Physical Security Guide». Kisi. https://pages.getkisi.com/physical-security-guide

2. Jonathan Wackrow. «Security Convergence: Addressing Evolving Cyber and Physical Security Threats». 2019. Teneo. https://www.teneo.com/vision-book/2019/security-convergence-addressing-evolving-cyber-and-physical-security-threats/

3. Pierluigi Paganini. «Modern Physical Security Awareness Is More Than Dumpster Diving [Updated 2019]». 27 agosto 2019. Infosec Institute. https://resources.infosecinstitute.com/modern-physical-security-awareness-is-more-than-dumpster-diving/#gref

4. Pierre Bourgeix. «2019. What's In & Out in Physical Security». 2019. Boon Edam. https://blog.boonedam.us/2019-whats-in-out-in-physical-security

5. Danny Bradbury. «Killer USB Breach Highlights Need For Physical Security». 23 aprile 2019. Infosec Magazine. https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/

6. «PCI DSS Quick Reference.» Luglio 2018. PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

7. «76% Security Professionals Face Cybersecurity Skills Shortage: Report.» 7 maggio 2020. CISOMAG. https://cisomag.eccouncil.org/security-leaders-lack-cybersecurity-skills/

8. «2019 Landscape Report: Hosted Security Adoption In Europe.» 2019. Morphean. https://morphean.com/whitepaper/

9. Catalin Cimpanu. «Crooks use digger to steal ATMs in Northern Ireland as ATM physical attacks rise across the EU.» 16 aprile 2019. ZDNet. https://www.zdnet.com/article/crooks-use-digger-to-steal-atms-in-northern-ireland-as-atm-physical-attacks-rise-across-the-eu/

10. Jovi Umawing. «Everything you need to know about ATM attacks and fraud: Part 1.» 29 maggio 2019. Malwarebytes Labs. https://blog.malwarebytes.com/101/2019/05/everything-you-need-to-know-about-atm-attacks-and-fraud-part-1/

11. «ATM Explosive Attacks - Dutch ATMs to be shut down overnight to counter ATM explosive attacks.» 19 dicembre 2019. European Association for Secure Transactions (EAST). https://www.association-secure-transactions.eu/dutch-atms-to-be-shut-down-overnight-to-counter-atm-explosive-attacks/

12. «2019 Payment Security Report», 2019 Data Breach Investigations Report. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

13. «2019 Payment Threats and Fraud Trends Report.» 9 dicembre 2019. Consiglio europeo per i pagamenti. https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

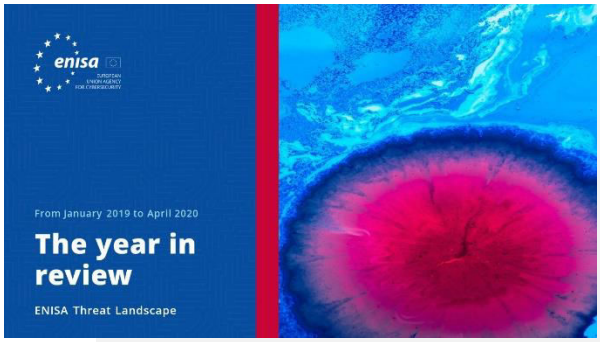
14. «2019 Eye on Privacy Report.» 2019. MediaPRO. https://pages.mediapro.com/Eye-on-Privacy-Report-2019-LP.html

15. «Report: 2020 State of Privacy and Security Awareness.» 2020. MediaPRO. https://www.mediapro.com/report-2020-state-of-privacy-security-awareness/

16. «Oracle and KPMG Cloud Threat Report.» 2019. ORACLE & KPMG. https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf


«Nel corso del prossimo decennio, i rischi legati alla cibersicurezza diventeranno più difficili da valutare e interpretare a causa della crescente complessità del panorama delle minacce, dell'ecosistema degli aggressori e dell'espansione della superficie di attacco.»
in ETL 2020

Correlati



Relazione sul panorama delle minacce dell'ENISA **L'anno in rassegna**

Una sintesi delle tendenze nella cibersicurezza per il periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Elenco delle prime 15 minacce**

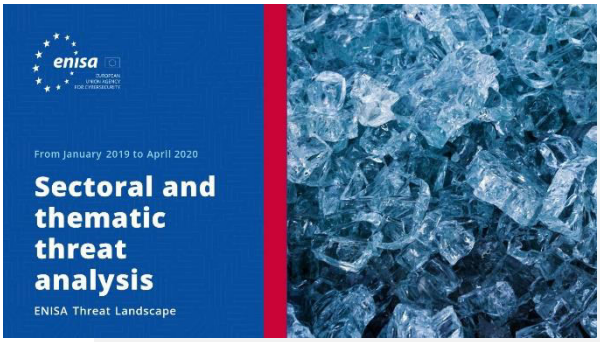
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Argomenti di ricerca**

Raccomandazioni su argomenti di ricerca di vari quadranti nella cibersicurezza e nell'intelligence sulle minacce informatiche.

LEGGI LA RELAZIONE



Relazione sul panorama delle minacce dell'ENISA **Analisi delle minacce settoriali e tematiche**

Analisi contestualizzata delle minacce tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Tendenze emergenti**

Principali tendenze nella cibersicurezza osservate tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Quadro generale dell'intelligence sulle minacce informatiche

Situazione attuale dell'intelligence sulle minacce informatiche nell'UE.

LEGGI LA RELAZIONE

Informazioni

_ L'agenzia

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in questo campo, aumenta l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili al seguente indirizzo: www.enisa.europa.eu.

Autori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) e *tutti i componenti del gruppo di portatori di interessi sulla CTI dell'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) e Thomas Hemker.

Redattori

Marco Barros Lourenço (ENISA) e Louis Marinos (ENISA).

Contatti

Per informazioni sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.
Per richieste dei media sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.

Saremmo lieti di ricevere il vostro feedback su questa relazione.
Dedicate un momento alla compilazione del questionario. Per accedere al modulo, fare clic qui.

Avvertenza legale

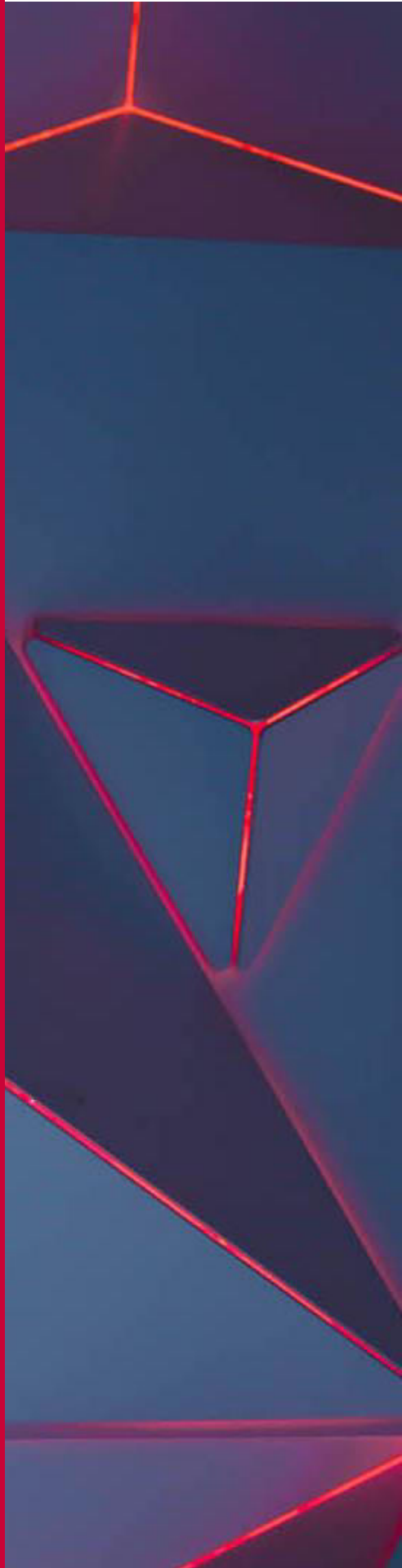
Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013. La presente pubblicazione non rappresenta necessariamente lo stato dell'arte e l'ENISA si riserva il diritto di aggiornarla di volta in volta.

Secondo necessità, sono state citate anche fonti di terze parti. L'ENISA non è responsabile del contenuto delle fonti esterne, quali i siti web esterni riportati nella presente pubblicazione.

La presente pubblicazione è unicamente a scopo informativo. Deve essere accessibile gratuitamente. L'ENISA, o chiunque agisca in suo nome, declina ogni responsabilità per l'uso che può essere fatto delle informazioni di cui alla presente pubblicazione.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu