enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Minaccia interna

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Una minaccia interna è un'azione che può portare a un incidente, compiuta da una persona o da un gruppo di persone affiliate alla potenziale vittima o che lavorano per la medesima. Esistono diversi modelli associati alle minacce interne. Uno molto noto (definito anche «abuso dei privilegi») si profila quando soggetti esterni collaborano con attori interni per ottenere accesso non autorizzato agli asset. Gli insider possono causare un danno involontariamente, per negligenza o per mancanza di conoscenza. Dal momento che questi insider godono spesso di fiducia e privilegi, oltre a conoscere le politiche, i processi e le procedure dell'organizzazione, è difficile distinguere tra accesso legittimo, malevolo ed erroneo ad applicazioni, dati e sistemi.[1]

I cinque tipi di minaccia interna possono essere definiti secondo le motivazioni e gli obiettivi:

a) lavoratori negligenti che trattano impropriamente i dati, violano le politiche di utilizzo e installano applicazioni non autorizzate;

b) agenti interni che rubano informazioni per conto di terzi;

c) dipendenti insoddisfatti che cercano di danneggiare la loro organizzazione;

d) insider malintenzionati che sfruttano i privilegi esistenti per rubare informazioni a scopo di guadagno personale;

e) terzi irresponsabili che compromettono la sicurezza attraverso l'intelligence, l'uso improprio o l'accesso a un asset o il suo utilizzo per finalità malevole.

Tutti e cinque i tipi di minacce interne devono essere oggetto di costante studio, in quanto il riconoscimento della loro esistenza e del loro modus operandi dovrebbe definire la strategia dell'organizzazione in tema di sicurezza e protezione dei dati.

Risultati

Il 65%_ **dell'impatto prodotto da minacce interne comprende il danno alla reputazione e alle finanze dell'organizzazione[12]**

L'88%_ **delle organizzazioni interpellate riconosce che le minacce interne sono motivo di allarme[10]**

11,45_ **milioni di euro è il costo medio annuo degli incidenti di cibersicurezza causati da un soggetto interno all'organizzazione[8]**

Il 40%_ **delle organizzazioni interpellate si ritiene vulnerabile per quanto riguarda la divulgazione di informazioni aziendali riservate[11]**

Kill chain

Minacce interne

Reconnaissance (Ricognizione)	Weaponisation (Armamento)	Delivery (Consegna)	Exploitation (Sfruttamento)

Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo

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

Descrizione

_Il denaro detta le regole

A causa del costo crescente di altri vettori di attacco, gli aggressori sono disposti a offrire grandi quantità di denaro agli insider. Il prezzo di un insider varia a seconda della sua posizione in azienda, dell'azienda stessa, del tipo e della complessità del servizio richiesto, del tipo di dati che vengono esfiltrati e del livello di sicurezza applicato dall'azienda. Tra le modalità con cui gli aggressori reclutano gli insider figurano: (1) la semplice pubblicazione di un'offerta su forum e la proposta di una ricompensa per determinate informazioni; (2) la presentazione delle loro azioni in modo che i dipendenti non si rendano conto di agire illegalmente, divulgare informazioni personali o intraprendere attività di insider e (3) il ricatto.[4]

_Azioni criminali urbi et orbi

Un ex ingegnere del software di un fornitore di servizi cloud ha approfittato di un errore di configurazione del firewall delle applicazioni web per accedere a più di 100 milioni di account e dati di carte di credito dei clienti. L'azienda ha poi corretto la vulnerabilità e ha dichiarato che «né i numeri di carta di credito né le credenziali di accesso erano stati compromessi». Questo caso di minaccia interna è particolarmente interessante perché l'ex dipendente trasformatosi in hacker non si è preoccupato di nascondere l'identità. Ha infatti condiviso il metodo di hacking con i colleghi di Capital One su un servizio di chat, ha pubblicato le informazioni su GitHub (con nome e cognome) e se ne è perfino vantato sui social media. Questo tipo di comportamento è un fenomeno che gli psicologi definiscono «trapelamento» (leakage), in cui gli insider che tramano per arrecare il danno rivelano i loro piani. Capital One prevede che la violazione costerà fino a 150 milioni di dollari USA (circa 127 milioni di euro)[5]

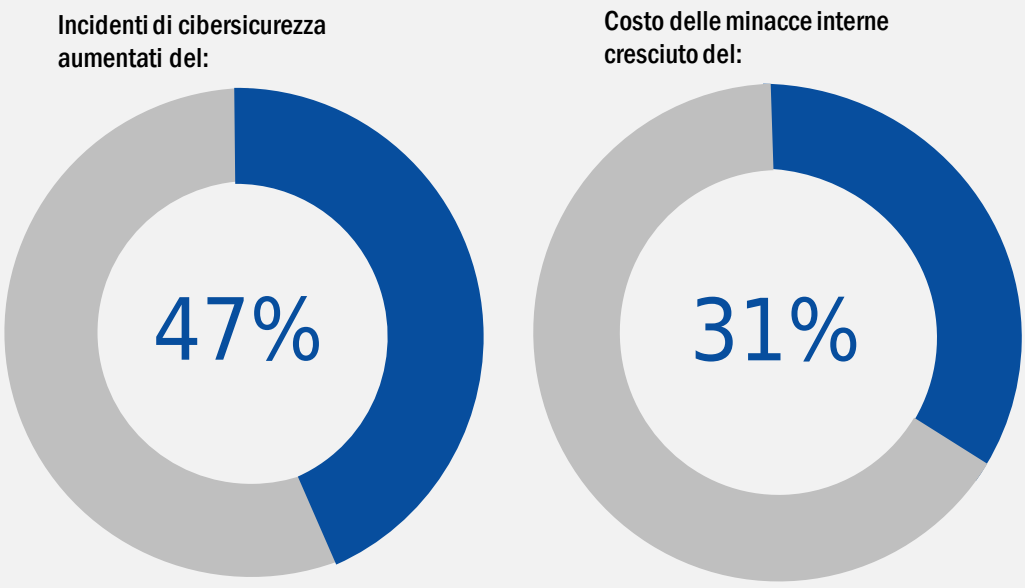


Figura 2. Incidenti e andamento dei costi. Fonte: Observeli[8]

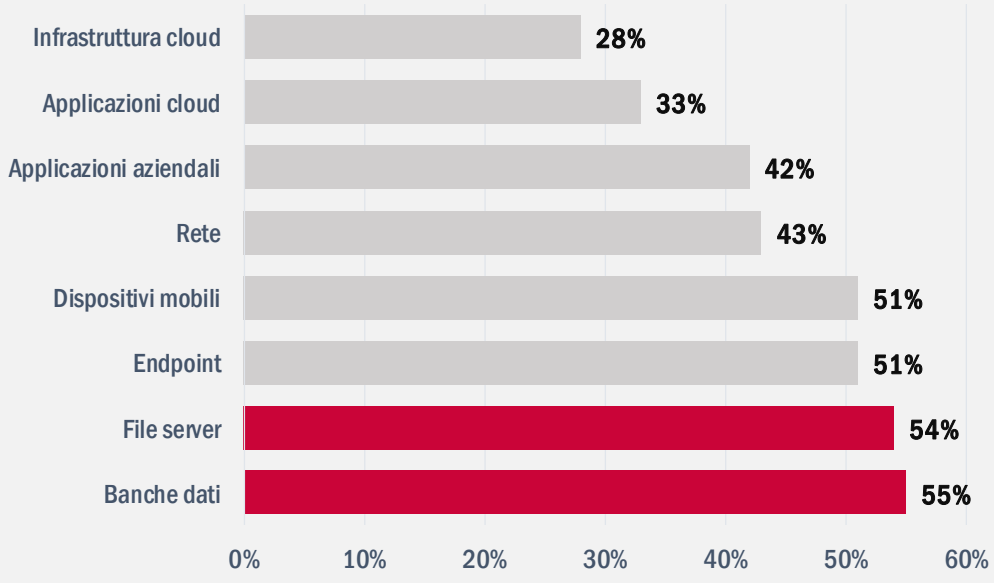


Figura 2. Asset IT vulnerabili alle minacce interne. Fonte: Help Systems[9]

Vettori di attacco

_Come

Una recente indagine[14] ha rivelato che i gruppi sono le minacce interne più pericolose nelle aziende e in altre organizzazioni.

Secondo gli esperti di cibersicurezza[15], il phishing (38%) è la principale vulnerabilità nel caso di minacce interne non intenzionali. Più in basso nella classifica si collocano lo spear phishing (21%), le password deboli o riutilizzate (16%), gli account orfani (10%) e la navigazione su siti sospetti (7%).

_ Area di impatto degli incidenti associati a minacce interne

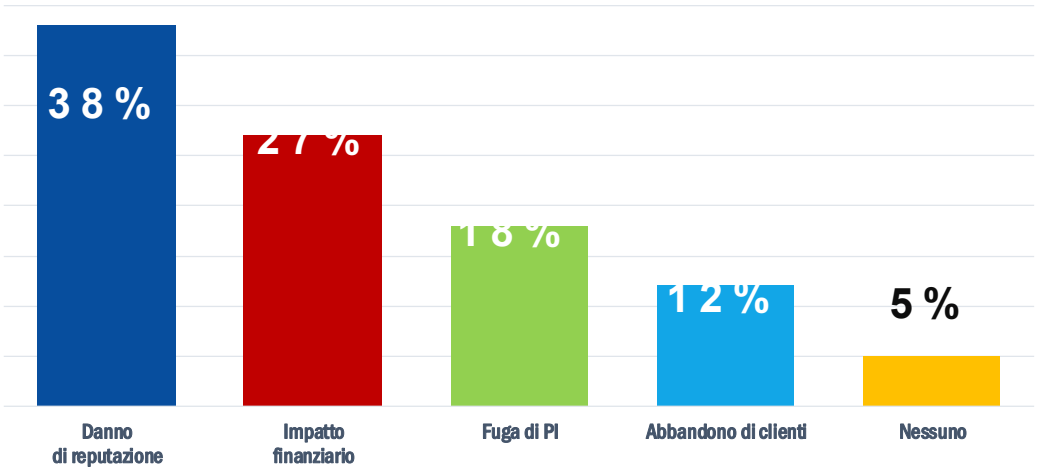


Figura 3 - Fonte: Egress[12]


«Gli insider possono causare un danno involontariamente, per negligenza o per mancanza di conoscenza».
in ETL 2020

Mitigazione

Azioni proposte

- Implementare una tecnologia di ispezione approfondita dei pacchetti (Deep Packet Inspection, DPI) per il rilevamento delle anomalie, che offra agli utenti industriali una piattaforma affidabile per monitorare il flusso dei comandi di controllo dei processi e dei dati telemetrici e per la protezione dalle minacce esterne. Allo stesso tempo, ciò mitiga il rischio di interferenze interne «avanzate» da parte di ingegneri, operatori SCADA o altro personale con accesso diretto ai sistemi.[16]
- Introdurre nella strategia e nelle politiche generali di sicurezza un piano di contromisure per le minacce interne. Questo piano comprende in genere un quadro di gestione del rischio, un piano di continuità operativa (BCP), un programma di ripristino in caso di disastro (Disaster Recovery Plan, DRP), politiche di gestione finanziaria e contabile e una gestione legale e normativa.[1]
- Creare un programma di sicurezza che preveda la conduzione di attività di ricerca proattiva delle minacce, la scansione delle vulnerabilità e i test di penetrazione, l'adozione di misure di sicurezza per il personale, l'impiego di misure di sicurezza fisica, l'implementazione di soluzioni di sicurezza della rete, l'utilizzo di soluzioni di sicurezza degli endpoint, l'applicazione di misure di sicurezza dei dati, l'impiego di misure di gestione delle identità e degli accessi, la creazione di capacità di gestione degli incidenti, il mantenimento di servizi di scienze forensi digitali e il ricorso a metodi di intelligenza artificiale (IA) per prevenire attacchi da parte di insider.
- Elaborare una politica di sicurezza sulle minacce interne basata sulla sensibilizzazione degli utenti, che rappresenta uno dei controlli più efficaci per questo tipo di minaccia informatica.
- Attuare controlli tecnici robusti. Le misure di sicurezza tradizionali tendono a concentrarsi sulle minacce esterne, ma non sono in genere efficaci nell'individuazione dei rischi interni che hanno origine nell'organizzazione. Per proteggere gli asset, attuare strumenti come la prevenzione della perdita di dati (Data Loss Prevention, DLP) per impedire l'esfiltrazione dei dati.[1]

- Ridurre il numero di utenti con privilegi e accesso alle informazioni sensibili. Se un dipendente non ha la necessità di accedere a determinate informazioni per svolgere il proprio lavoro, è consigliabile limitare ciò che può vedere, evitando così un accesso improprio.[17]
- Rafforzare l'ambiente digitale, ivi compreso l'irrigidimento della sicurezza della rete, dei sistemi, delle applicazioni, dei dati e degli account.[1]

Riferimenti bibliografici

1. «Insider Threat Report», 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

2. «Insider Threat Statistics Facts and Figures». Ekran System. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

3. «CyberEdge 2019 CDR Report» 2019. CyberEdge. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

4. «Corporate Security Predictions 2020». 2019. 3 dicembre 2019. Kapersky.

https://securelist.com/corporate-security-predictions-2020/95387/

5. «Famous Insider Threat Cases» Settembre 2019. Security Boulevard. https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

6. «The rise of insider threats: Key trends to watch» 2019. Tech Beacon.

https://techbeacon.com/security/rise-insider-threats-key-trends-watch

7. «Cost of Cybercrime study» 2019. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

8. «Cost of Insider Threats», 2020. Observer IT. https://www.observeit.com/cost-of-insider-threats/

9. «Cybersecurity Insiders 2019 Insider Threat Report», 2019. Help Systems.https://www.helpsystems.com/cta/2019-cybersecurity-insiders-insider-threat-report

10. «Forcepoint Insider threat Data Protection» 2017. Force Point.

https://www.forcepoint.com/sites/default/files/resources/files/brochure_insider_threat_data_protection_en.pdf

11. «State of Insider Threats in the Digital Workplace» 2019. Better Cloud. https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

12. «Insider Data Breach Survey 2019». 2019. Egress. https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

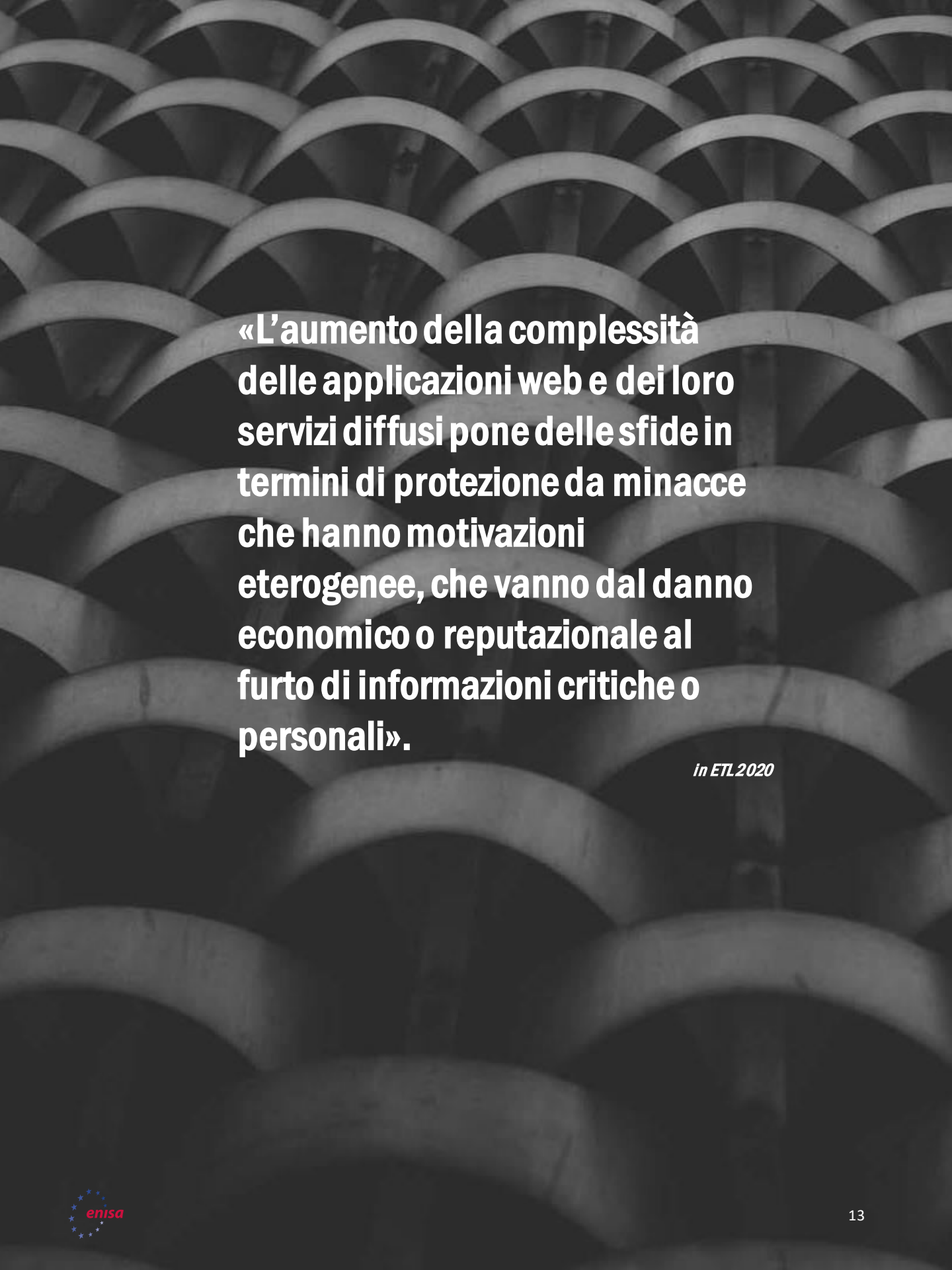
13. «Insider Threat Report». 2019. Nucleos Cyber. https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf

14. «Insider Threat Report». 2019. Haystax. https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

15. «Insider Threat Report». 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

16. «Kaspersky Industrial CyberSecurity: solution overview 2019». 2019. Kaspersky. https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

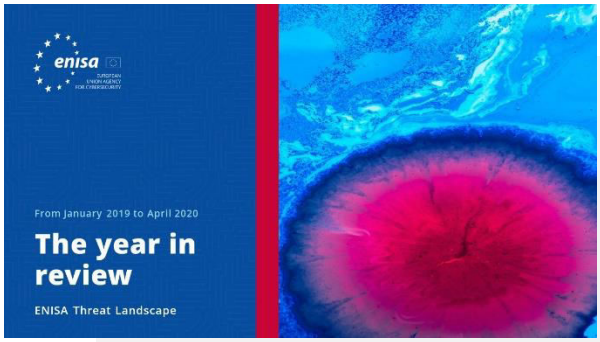
17. «Post-vacation cybersecurity tuneup: Get your company ready!». 1° settembre 2017. Panda. https://www.pandasecurity.com/mediacenter/adaptive-defense/cyber-security-get-company-ready/



«L'aumento della complessità delle applicazioni web e dei loro servizi diffusi pone delle sfide in termini di protezione da minacce che hanno motivazioni eterogenee, che vanno dal danno economico o reputazionale al furto di informazioni critiche o personali».

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

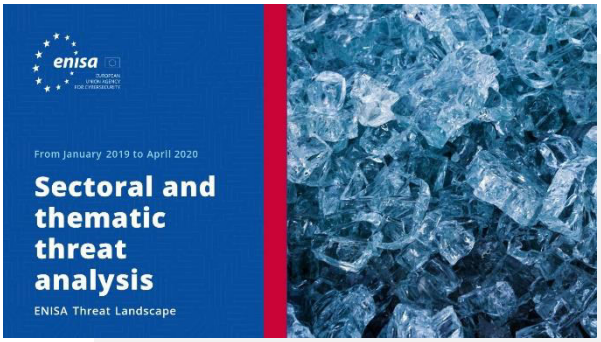
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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