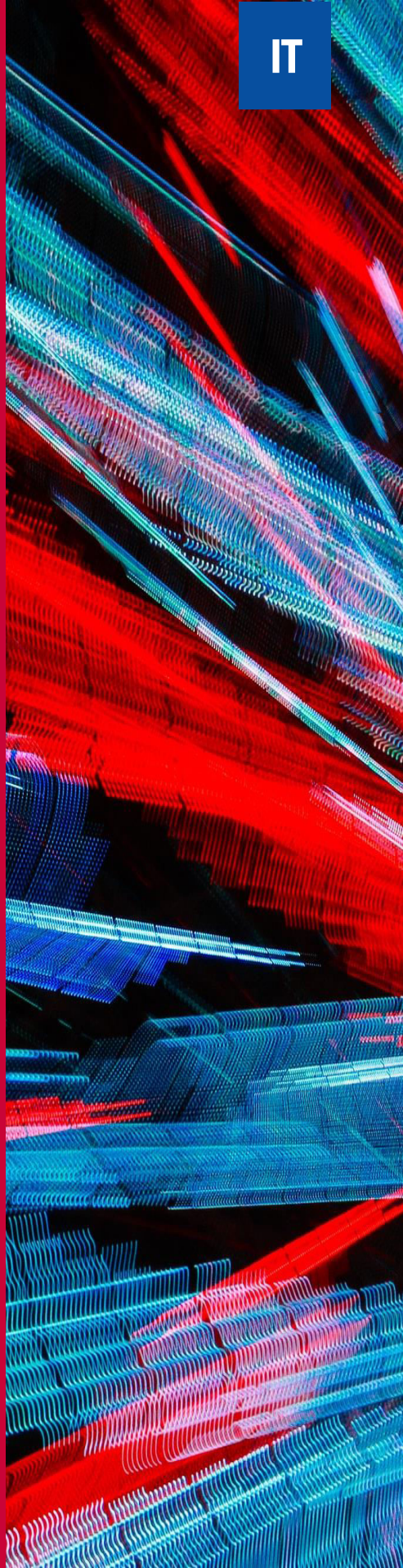
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT



Da gennaio 2019 ad aprile 2020

Tendenze emergenti

Panorama delle minacce analizzato dall'ENISA

Quadro generale

_Che cosa aspettarsi

Con l'inizio di un nuovo decennio possiamo aspettarci cambiamenti significativi nel modo di percepire e comprendere la cibersicurezza, ovvero la sicurezza del ciberspazio. Il ciberspazio è definito nella norma **ISO/IEC 27032:2012**[1] come il ***«complesso ambiente risultante dall'interazione di persone, software e servizi su Internet attraverso i dispositivi tecnologici e le reti ad essa collegati, ambiente che non esiste in forma fisica»***. La protezione di questo complesso ambiente diventerà ancora più impegnativa con l'aumento del numero di persone, dispositivi e sistemi connessi e dei processi e servizi eseguiti nella rete. Siamo anche più dipendenti dalla sua affidabilità, integrità, disponibilità e attendibilità per lavorare, relazionarci e svolgere molte delle nostre attività quotidiane. Con la crescita di questa dipendenza, emergeranno maggiori opportunità per gli attori malintenzionati di utilizzare il ciberspazio al fine di manipolare, intimidire, ingannare, molestare e frodare individui e organizzazioni. La tutela degli individui, delle imprese e delle organizzazioni quando utilizzano il ciberspazio tenderà a spostarsi, nel prossimo decennio, dalla tradizionale idea di sicurezza delle reti e dell'informazione (Network and Information Security, NIS) a un concetto più ampio, comprendente contenuti e servizi.

Nel corso dell'ultimo decennio la «quarta rivoluzione industriale» ha accelerato sensibilmente il ritmo del cambiamento, trasformando ciò che le persone fanno, il modo di farlo, le competenze richieste, il luogo in cui si svolge il lavoro, come si strutturano i rapporti lavorativi e le modalità di organizzare, distribuire e premiare il lavoro.

A causa dell'attuale pandemia di COVID-19, iniziamo il decennio con una nuova normalità e profondi cambiamenti nel mondo fisico e nel ciberspazio. In conseguenza del distanziamento sociale e delle misure di confinamento, le persone tenderanno a utilizzare lo spazio virtuale per comunicare, relazionarsi e socializzare. Questa nuova normalità introdurrà nuove sfide in tutta la catena del valore digitale e nel settore della cibersicurezza, in particolare.

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.

Sono troppe le variabili da considerare quando si tenta di rendere efficace la gestione del rischio informatico. Un fattore importante è l'eterogeneità tecnologica che sperimenta oggi la maggior parte delle organizzazioni. Un altro aspetto è la sofisticatezza degli strumenti, delle tattiche, tecniche e procedure (TTP) utilizzati dagli avversari per condurre gli attacchi. Gli attori malintenzionati adattano e regolano le TTP all'ambiente della vittima, secondo le necessità e collaborando con altri per raggiungere i loro obiettivi.

La definizione di una posizione di rischio, la gestione dei dati, l'applicazione di metriche pertinenti e la risposta al cambiamento sono ostacoli alla creazione di una strategia di governance del rischio cibernetico efficace. **Nel corso del prossimo decennio serviranno nuovi approcci per abbandonare l'analisi per compartimenti stagni e avvicinarsi a un tipo a matrice di fattori, variabili e condizioni interconnessi**. Ciò costituisce una sfida significativa per molte organizzazioni che cercano di proteggere la loro infrastruttura, le attività operative e i dati da avversari più forti e dotati di equipaggiamento e risorse migliori.

Tendenze emergenti

Dieci sfide per la cibersicurezza

01_Gestire rischi sistemici e complessi. Il rischio cibernetico è caratterizzato dalla velocità e dalle dimensioni della sua propagazione, nonché dal potenziale intento degli attori delle minacce. L'interconnessione di vari sistemi e reti consente una diffusione ampia e rapida degli incidenti informatici, rendendo più difficile la valutazione e la mitigazione dei rischi cibernetici.

02_Rilevamento dell'Adversarial AI.
Il rilevamento delle minacce che sfruttano l'IA per lanciare un attacco o evitare di essere individuate costituirà una sfida importante per il futuro dei sistemi di ciberdifesa.[14]

03_Riduzione degli errori involontari.
Con il crescente numero di sistemi e dispositivi connessi alla rete, gli errori involontari continuano ad essere una delle vulnerabilità più sfruttate negli incidenti di cibersicurezza. Nuove soluzioni finalizzate alla riduzione di tali errori forniranno un importante contributo al contenimento del numero di incidenti.

04_Minacce dalla catena di fornitura e da terzi.
La catena di fornitura diversificata che caratterizza il settore tecnologico attuale offre agli attori delle minacce nuove opportunità per approfittare di questi sistemi complessi e per sfruttare le diverse vulnerabilità introdotte da un ecosistema eterogeneo di fornitori terzi.[16]

05_Orchestrazione e automazione della sicurezza.
L'intelligence sulle minacce informatiche e gli analytics comportamentali acquisiranno importanza con l'automazione dei processi e delle analisi. Investire nell'automazione e nell'orchestrazione permetterà
ai professionisti del settore di investire nella progettazione di
strategie di cibersicurezza più robuste.

06_Riduzione dei falsi positivi. Questa promessa a lungo attesa è fondamentale nel futuro dell'industria della cibersicurezza e nella lotta contro l'affaticamento dovuto al sovraccarico di allarmi (alarm fatigue).

07_Strategie di sicurezza «zero trust». Con l'aumento della pressione sui sistemi IT generato dalle nuove esigenze aziendali come il telelavoro, la digitalizzazione del modello di business e l'espansione incontrollata dei dati, una strategia di «zero trust» è ritenuta da molti decisori la soluzione de facto per proteggere le risorse aziendali.

08_Errori nella migrazione delle imprese verso il cloud. Dato l'elevato numero di aziende che trasferiscono i loro dati verso soluzioni basate sul cloud, aumenteranno gli errori di configurazione, esponendo i dati a potenziali violazioni. I fornitori di servizi cloud affronteranno il problema con l'implementazione di sistemi in grado di identificare questo tipo di errori automaticamente.

09_Minacce ibride. Il nuovo *modus operandi* prevede l'adozione di minacce dal mondo fisico e virtuale. La diffusione di disinformazione o di notizie false, ad esempio, è un elemento chiave del panorama delle minacce ibride. EUvsDisinfo[15] è il progetto di punta della task force East StratCom del Servizio europeo per l'azione esterna, istituito per affrontare la minaccia costituita dalla disinformazione.

10_Aumenterà l'attrattiva delle infrastrutture cloud come bersaglio. Il crescente affidamento sulle infrastrutture cloud pubbliche farà aumentare il rischio di indisponibilità. L'errata configurazione delle risorse cloud è tuttora la prima causa di attacchi al cloud, anche se gli attacchi mirati direttamente ai fornitori di servizi cloud stanno acquisendo popolarità tra gli hacker.

Tendenze emergenti

_ Spesa per la cibersicurezza

Secondo Gartner[17], molti consigli di amministrazione esigeranno un miglioramento dei dati e della comprensione dei rendimenti, dopo anni di intensi investimenti nella cibersicurezza. Ciò a causa, soprattutto, di una crescita della spesa per la cibersicurezza in proporzione agli investimenti effettuati nelle nuove tecnologie. Secondo un rapporto di IDC[22], la spesa per la cibersicurezza ha raggiunto 103 miliardi di dollari USA (circa 87,5 miliardi di EUR) nel 2019, registrando un aumento del 9,4% rispetto all'anno precedente. I responsabili della sicurezza saranno presto posti sotto la lente di ingrandimento per i risultati conseguiti da anni di investimenti e sono essenziali per mantenere dati migliori riguardo a tali risultati.

_ L'intelligence sulle minacce informatiche aiuterà a definire le strategie di cibersicurezza

L'intelligence sulle minacce informatiche (Cyber Threat Intelligence, CTI)[7] mira ad aiutare le organizzazioni ad essere più preparate, grazie a una migliore conoscenza del panorama delle minacce. Anziché affidarsi esclusivamente alle informazioni generate dai sistemi o dai feed interni (ciò che si sa riguardo a quanto è già noto), l'efficacia della CTI sarà determinata dal conoscere il *perché*, il *come* e il *che cosa* è sconosciuto al team della cibersicurezza. La proposta di valore di qualsiasi capacità o programma di CTI è migliorare la preparazione dell'organizzazione a proteggere gli asset critici da minacce sconosciute.

Conoscere il panorama delle minacce

Con la tendenziale crescita dell'automazione e dell'orchestrazione della cibersicurezza, **i team di sicurezza informatica dedicheranno meno tempo alle attività di monitoraggio e più tempo alle attività di preparazione.** Una capacità di CTI ben concepita può fornire una conoscenza contestualizzata e utilizzabile delle minacce, per informare i portatori di interessi strategici, operativi e tattici in tutta l'organizzazione. In termini pratici, una capacità di CTI deve porsi l'obiettivo di rispondere alle seguenti domande, considerando le esigenze dei portatori di interessi e il contesto e l'ambiente dell'organizzazione:

- Qual è la superficie d'attacco?
- Quali sono gli asset più preziosi e il terreno cibernetico?
- Quali sono le vulnerabilità più critiche?
- Quali sono i vettori di attacco più utilizzati?
- Come si comportano e operano in genere gli avversari?
- Come si presenta il panorama delle minacce per:
    - il settore e il tipo di attività in cui opera l'organizzazione?
    - l'ambiente tecnologico adottato dall'organizzazione?
- Che cosa occorre fare per mitigare i rischi derivanti da queste minacce e chi se ne deve occupare?

Carenza di competenze nella cibersicurezza

La mancanza di professionisti tecnici altamente qualificati costituisce già un problema per l'ambizione di digitalizzazione dell'Europa. Secondo uno studio[23], oltre il 70% delle imprese europee riferisce che la mancanza di competenze ostacola le strategie di investimento, mentre il 46% lamenta difficoltà a coprire i posti vacanti a causa della carenza di competenze in settori essenziali come la cibersicurezza.

Tendenze emergenti

_ *Cinque* tendenze riguardo alle minacce informatiche

01_ **Il malware sale di livello.** I ceppi delle famiglie di malware vengono potenziati in nuove versioni con funzionalità e meccanismi di distribuzione e propagazione aggiuntivi. Emotet, ad esempio, un malware originariamente concepito come trojan bancario nel 2014, è diventato uno dei più efficaci distributori di malware del 2019.[2]

02_ **Le minacce interesseranno i dispositivi mobili.** Gli utenti sono sempre più dipendenti dai dispositivi mobili per proteggere gli account più sensibili. Ne è un esempio il ricorso all'autenticazione a due fattori (2fa) legata a un autenticatore basato su app o tramite messaggio di testo. Con la piena espansione del malware ai dispositivi mobili, le app fraudolente, il SIMJacking e l'exploit dei sistemi operativi rendono questi dispositivi l'anello più debole e perciò estremamente vulnerabili agli attacchi.

03_ **Gli aggressori utilizzano nuovi tipi di file, come i file immagine disco (ISO e IMG), per la diffusione del malware.** I file DOC, PDF, ZIP e XLS restano l'allegato più comunemente impiegato per la diffusione di malware, ma altri tipi si stanno affermando. In alcune campagne di distribuzione di AgentTesla InfoStealer e NanoCore RAT è stato rilevato l'utilizzo del tipo di file immagine nel 2019.

04_ **Aumento degli attacchi di ransomware mirati e coordinati.** Nel 2019 abbiamo assistito a un'escalation di attacchi ransomware mirati e sofisticati presso il settore pubblico, le organizzazioni sanitarie e industrie specifiche in cima alla classifica. Gli aggressori dedicano più tempo alla raccolta di informazioni sulle loro vittime, sapendo esattamente cosa codificare, realizzando la massima perturbazione e riscatti più elevati.

05_ **Si diffonderanno gli attacchi di «credential stuffing».** Si moltiplicherà il «credential stuffing», ovvero l'iniezione in automatico di combinazioni di nome utente e password rubate attraverso richieste di login automatizzate su larga scala dirette contro un'applicazione web, come conseguenza di un decennio caratterizzato da un numero anomalo di violazioni dei dati e da migliaia di miliardi di record di dati personali sottratti.


«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

Tendenze emergenti

Dieci tendenze emergenti nei vettori di attacco

01_ Gli attacchi saranno massicciamente distribuiti, con breve durata e vasto impatto

L'intento di tali attacchi è colpire il maggior numero possibile di dispositivi per rubare informazioni personali o bloccare l'accesso ai dati crittografando i file.

02_ Attacchi finemente mirati e persistenti saranno meticolosamente pianificati, con obiettivi ben definiti e a lungo termine

Gli attori malintenzionati pianificano questo tipo di attacchi per raggiungere dati di alto valore, come informazioni finanziarie, proprietà intellettuale e industriale, segreti commerciali, informazioni classificate, ecc.

03_ Gli attori malintenzionati utilizzeranno le piattaforme digitali in attacchi mirati

Gli attori malintenzionati sonderanno il potenziale delle piattaforme digitali a supporto di attacchi mirati (ad esempio social media, giochi, messaggistica, streaming, ecc.). Dal furto di dati personali per gli attacchi di spear phishing alla vasta distribuzione di malware, le piattaforme digitali con un elevato numero di abbonati sono vettori di attacco efficienti, sempre più sfruttate dagli attori malintenzionati.

04_ Aumenterà lo sfruttamento dei processi aziendali

Con la crescita dell'automazione e la diminuzione dell'intervento umano, i processi aziendali possono essere intenzionalmente alterati al fine di generare utili per un aggressore. Nota come Business Process Compromise (BPC), questa tecnica di compromissione dei processi aziendali è spesso sottovalutata dagli specialisti di ingegneria di processo, a causa dell'assenza di una corretta valutazione del rischio.

05_ La superficie di attacco continuerà a espandersi

La posta elettronica non è più il principale e unico strumento e più importante vettore di attacco per il phishing. Gli attori malintenzionati utilizzano ora altre piattaforme per comunicare con le vittime e indurle ad aprire pagine web compromesse. Una nuova tendenza sta emergendo con l'uso di SMS, WhatsApp, SnapChat e piattaforme di messaggistica sui social media.

06_ Le vulnerabilità del telelavoro saranno sfruttate attraverso i dispositivi domestici

Con l'aumento del numero di persone che lavorano a distanza e che collegano i loro dispositivi alle reti aziendali, crescerà il rischio di aprire nuovi punti di ingresso per gli aggressori. Con la pandemia di COVID-19, questa tendenza spronerà i responsabili dell'IT a rafforzare le politiche di sicurezza e ad apportare cambiamenti urgenti all'infrastruttura informatica.

07_ Gli aggressori arriveranno meglio preparati

Gli aggressori scelgono i loro obiettivi con attenzione, effettuano ricognizioni rispetto a dipendenti specifici e li prendono di mira con attacchi di spear phishing per ottenere credenziali utilizzabili per colpire l'organizzazione. Una volta che gli aggressori hanno accesso a una singola macchina, possono utilizzare strumenti per test di penetrazione, come Mimikatz, per raccogliere e sfruttare le credenziali con privilegi elevati.

08_ Le tecniche di offuscamento diventeranno più sofisticate

Gli attori malintenzionati si evolvono costantemente per rendere le minacce più efficaci e meno rilevabili. Anubis, un trojan bancario e bot per Android, è stato distribuito spacciandosi per innocua app, soprattutto attraverso Google Play Store.[1]

09_ Aumenterà lo sfruttamento automatizzato delle vulnerabilità dei sistemi privi di patch e delle applicazioni fuori produzione

L'aumento anomalo del traffico Telnet verso la porta 445 osservato nel 2019 ha rivelato l'espansione di worm e di exploit come Eternal Blue. Telnet, che non è più utilizzato se non nel campo dei dispositivi IoT, ha registrato i maggiori volumi durante tale periodo.

10_ Le minacce informatiche si spostano verso l'edge computing

I dispositivi edge sono installati ai confini tra le reti interconnesse. Abbiamo osservato una crescita tendenziale degli attacchi mirati a questi dispositivi, come router, switch e firewall, con un impatto significativo sulle imprese e sull'ecosistema digitale connesso.

Riferimenti bibliografici

1. «ISO/IEC 27032:2012». ISO. https://www.iso.org/standard/44375.html

2. «Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk.» 2 aprile 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

3. «Understanding the relationship between Emotet, Ryuk and TrickBot.» 14 aprile 2019. Intel471. https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

4. «Investigating WMI Attacks" 9 febbraio 2019. SANS. https://www.sans.org/blog/investigating-wmi-attacks/

5. «RDP Abuse and Swiss Army Knife Tool Used to Pillage, Encrypt and Manipulate Data» 18 dicembre 2019. Bitdefender. https://labs.bitdefender.com/2019/12/rdp-abuse-and-swiss-army-knife-tool-used-to-pillage-encrypt-and-manipulate-data/

6. «Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook» 10 luglio 2019. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

7. «This is how we might finally replace passwords» 27 maggio 2019. C | Net. https://www.cnet.com/news/this-is-how-we-might-finally-replace-passwords/

9. «Authentication standards to help reduce the world's over-reliance on passwords.» FIDO. https://fidoalliance.org/overview/

10. «How Much Cyber Sovereignty is Too Much Cyber Sovereignty?» 3 ottobre 2019. Council on Foreign Relations. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

11. «Conceptualising Cyber Arms Races». 2016. NATO. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

12. «Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training» 2018. UNESCO. https://en.unesco.org/fightfakenews

13. «The Big Connect: How Data Science is Helping Cybersecurity». 12 giugno 2019. Info Security Group. https://www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/

14. «Are You Ready For The Age Of Adversarial AI? Attackers Can Leverage Artificial Intelligence Too». 9 gennaio 2020. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/#2a76dee14703

15. https://euvsdisinfo.eu/

16. «FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains». 21 febbraio 2020. Bitsight. https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

17. «Gartner Identifies the Top Seven Security and Risk Management Trends for 2019». 5 marzo 2019. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

18. «Android banking trojan.» 3 ottobre 2019. Cyare. https://cyware.com/news/exploring-the-nature-and-capabilities-of-anubis-android-banking-trojan-6ea7dec4

19. «5 Top Trends for Mobile Cyber Security in 2020». 9 gennaio 2020. Corrata. https://corrata.com/5-top-trends-for-mobile-cyber-security-in-2020/

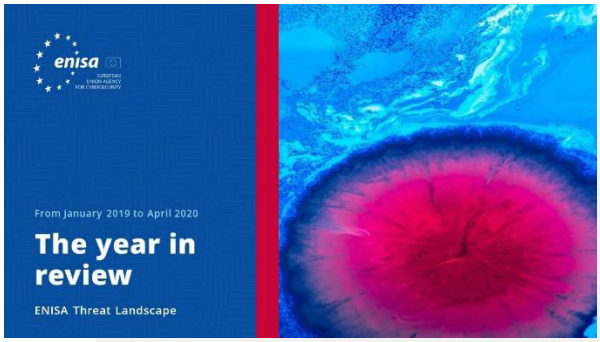
20. «Malicious Attachments Remain a Cybercriminal Threat Vector Favorite». 27 agosto 2020. Threat Post. https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/

21. «10 trends shaping the future of work». Ottobre 2019. EPSC. https://op.europa.eu/en/publication-detail/-/publication/e77a1580-0cf5-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-121729338

22. «Global security spending to top $103 billion in 2019, says IDC», 20 marzo 2019. ZDNet. https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

23. «Insights into skills shortages and skills mismatch. learning from Cedefop's European skills and jobs survey». 2018. CEDEFOP. https://www.cedefop.europa.eu/files/3075_en.pdf

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

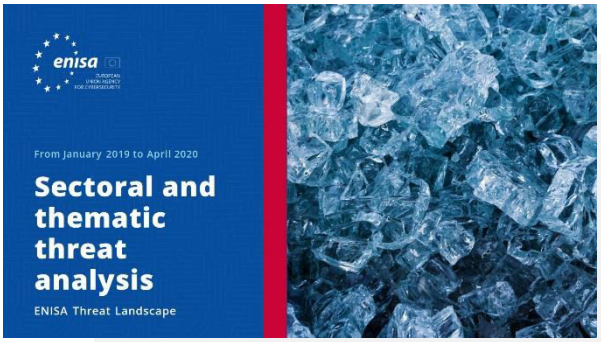
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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.

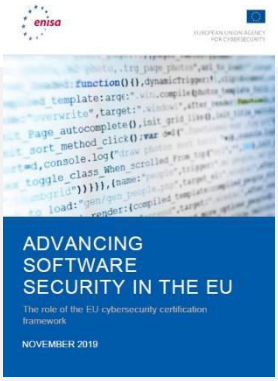
LEGGI LA RELAZIONE

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

Altre pubblicazioni



Advancing Software Security in the EU (Promuovere la sicurezza del software nell'UE)

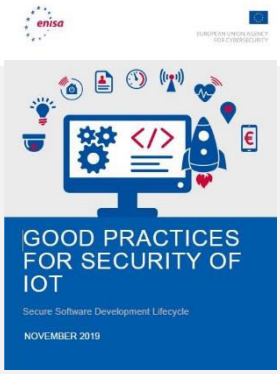
Presenta gli elementi chiave della sicurezza del software e fornisce un quadro conciso degli approcci e degli standard esistenti più pertinenti nel panorama dello sviluppo di software sicuro.

LEGGI LA RELAZIONE

ENISA good practices for security of Smart Cars (Buone pratiche dell'ENISA per la sicurezza delle auto intelligenti)

Buone pratiche per la sicurezza delle auto intelligenti, ovvero i veicoli connessi e (semi-) autonomi, per migliorare l'esperienza degli utilizzatori e accrescere la sicurezza delle auto .

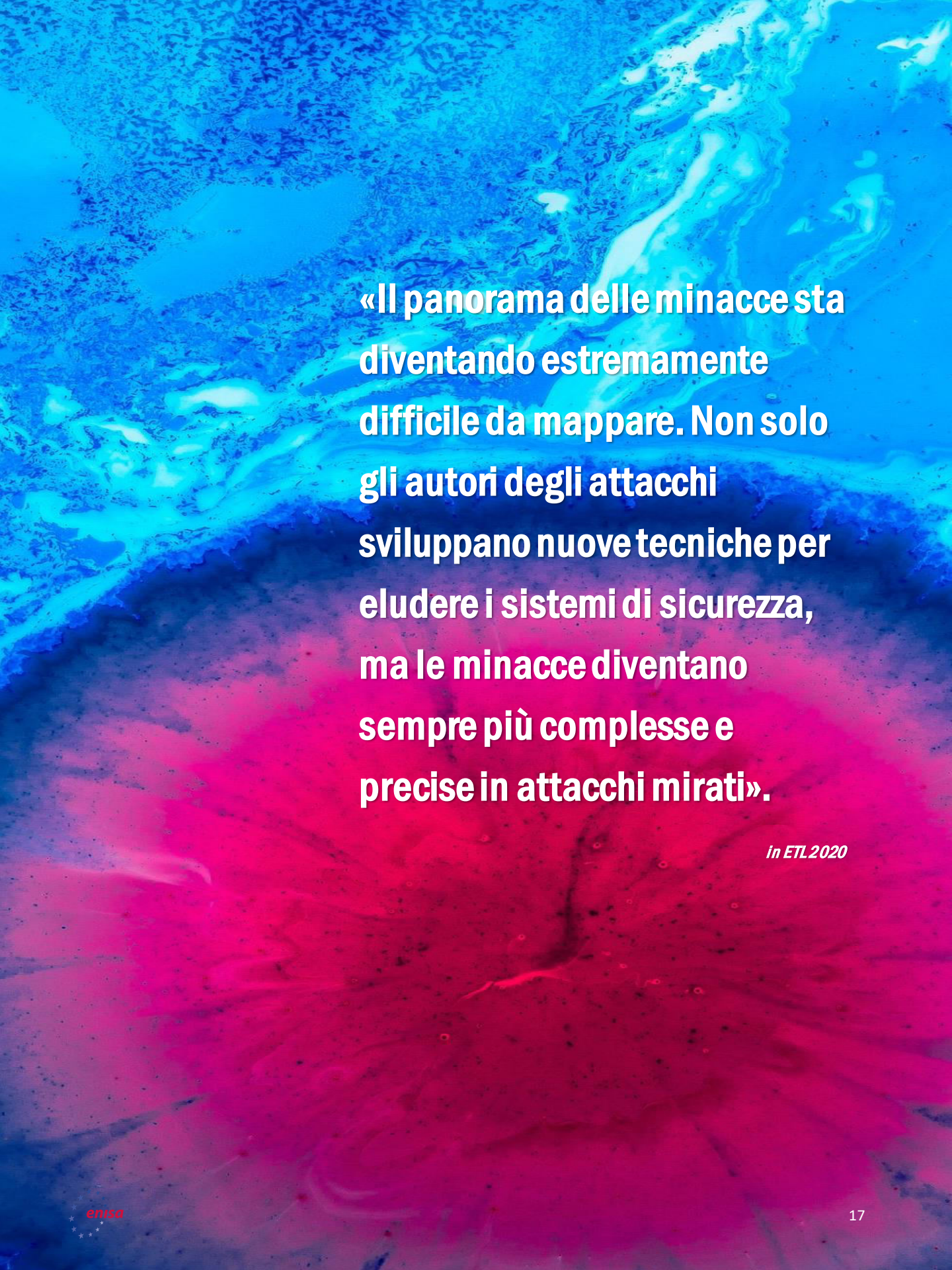
LEGGI LA RELAZIONE



Good Practices for Security of IoT - Secure Software Development Lifecycle (Buone pratiche per la sicurezza dell'Internet degli oggetti - Ciclo di vita dello sviluppo di software sicuro)

Sicurezza dell'IoT, con particolare attenzione alle linee guida di sviluppo del software.

LEGGI LA RELAZIONE


«Il panorama delle minacce sta diventando estremamente difficile da mappare. Non solo gli autori degli attacchi sviluppano nuove tecniche per eludere i sistemi di sicurezza, ma le minacce diventano sempre più complesse e precise in attacchi mirati».
in ETL 2020

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

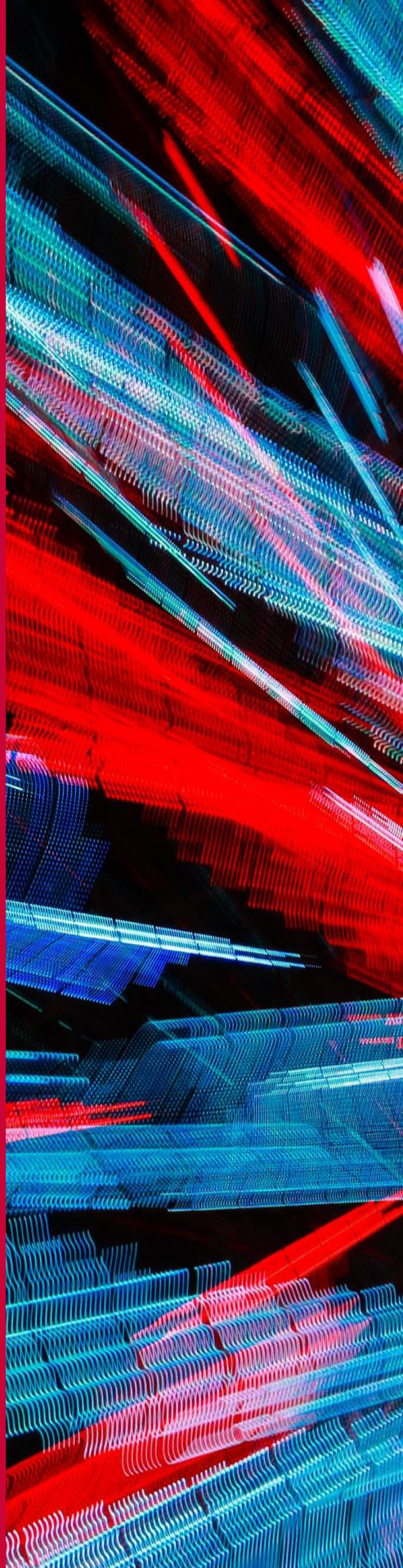
Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013. 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