IT

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Da gennaio 2019 ad aprile 2020

Argomenti di ricerca

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Nuovi concetti e idee stanno evolvendosi nel settore della cibersicurezza grazie alle attività di ricerca e innovazione condotte dal mondo accademico, dall'industria e dai professionisti in tutto il mondo. Si tratta di passi importanti, poiché il ritmo dell'innovazione da parte degli avversari (ad esempio gli attori malevoli) è più elevato rispetto a quello degli specialisti della cibersicurezza che devono trovare soluzioni per dissuaderli. Di fatto, a parte l'igiene e la formazione di base in materia di sicurezza informatica, investire nella ricerca e nell'innovazione è l'opzione più valida affinché chi è chiamato alla difesa si avvicini a ciò che è necessario per migliorare la sicurezza del ciberspazio. In questa relazione vengono messi in luce alcuni dei più importanti argomenti di ricerca e innovazione in tema di cibersicurezza esplorati nell'UE e nel mondo.

Migliore comprensione della dimensione umana

La sicurezza informatica è ancora vista come la pratica di proteggere le reti, i sistemi informativi e i dati (NIS). Tale definizione deve essere ulteriormente ampliata al di là delle questioni tecniche per includere i timori di natura sociale, comportamentale ed economica e i diversi ruoli svolti dalle parti coinvolte. Ciò dovrebbe costituire una priorità nelle future discussioni sulla ricerca e sull'innovazione nella cibersicurezza. Una migliore comprensione della dimensione umana è fondamentale per definire qualsiasi strategia di sicurezza informatica, in modo che le decisioni in materia siano adottate per soddisfare le relative esigenze, competenze e aspettative.

Ricerca e innovazione nella cibersicurezza

Nel corso del 2019 abbiamo osservato un aumento del numero di laboratori di prova e poligoni virtuali[1] che si sono resi disponibili in locale e in offerte cloud. Si tratta di risorse essenziali per consentire ai ricercatori di simulare attacchi, sviluppare scenari di exploit, ottenere dati operativi e sperimentare strategie di difesa in un ambiente virtuale polivalente. Gli ambienti di prova esistenti non sono tuttavia in grado di replicare molte vulnerabilità che in genere compromettono la sicurezza, come ad esempio i fattori umani e ingegneristici. Per migliorare l'efficienza, è importante fare ricerca e innovazione riguardo alla portata e all'accuratezza di questi laboratori di prova e proporre nuove soluzioni tecniche.

Quadro generale

Sicurezza del 5G

Il lancio delle reti mobili 5G è iniziato in alcuni paesi nel 2019, ma si prevede un aumento del numero di installazioni nel 2021. Questa nuova generazione di comunicazioni mobili è di capitale importanza per il progresso sociale ed economico dell'Unione europea. Pertanto, la ricerca e lo sviluppo futuri di soluzioni di sicurezza 5G rivestono un ruolo essenziale per la sostenibilità e l'affidabilità di questa tecnologia. Nel 2019 l'ENISA ha pubblicato un panorama delle minacce per le reti 5G, esaminando alcuni aspetti critici della sicurezza legati a questa tecnologia emergente.[2] I temi chiave nella ricerca e nell'innovazione della sicurezza del 5G devono tenere in considerazione i punti di seguito delineati.

- La ricerca e lo sviluppo di controlli di sicurezza che comprendano la protezione della rete, degli elementi fisici e dei livelli di dati, fornendo così una soluzione di protezione multi-livello. Con le reti 5G i dati saranno collocati in server cloud centralizzati, nodi Fog intermedi e dispositivi edge, aumentando la complessità di attuazione di una soluzione di sicurezza.

- La ricerca e lo sviluppo di standard e requisiti per i controlli di sicurezza da implementare su reti interconnesse con più proprietari, topologie, operatori e una varietà di dispositivi e livelli di rete diversificati.

- La ricerca e lo sviluppo di capacità di gestione delle chiavi, che consentano un'interoperabilità sicura tra i nodi che collegano dispositivi edge e IoT con risorse limitate. Questa capacità deve prevedere tecniche efficaci di controllo degli accessi, autenticazione, crittografia e gestione delle chiavi per i nodi con risorse limitate.

Progetti di ricerca e innovazione in tema di cibersicurezza nell'UE

- L'UE è al lavoro per creare un progetto pilota per una rete di competenze nella cibersicurezza. CONCORDIA[3], ECHO[4], SPARTA[5] e CyberSec4Europe[6] sono i quattro progetti pilota vincitori dell'invito del 2018 a presentare proposte per la sicurezza informatica nel quadro di Orizzonte 2020 al fine di «istituire e gestire un progetto pilota per una rete europea di competenze nel settore della cibersicurezza ed elaborare una tabella di marcia comune europea per la ricerca e l'innovazione in materia di cibersicurezza». L'UE prevede di rafforzare la propria capacità di cibersicurezza e di affrontare le future sfide in questo campo con questi quattro progetti pilota, per un mercato unico digitale europeo più sicuro.
- L'UE stanzia 38 milioni di euro per la protezione delle infrastrutture critiche dalle minacce informatiche. La Commissione europea ha annunciato l'impegno di oltre 38 milioni di euro tramite Orizzonte 2020 per il programma di ricerca e innovazione dell'UE. Il programma è destinato a sostenere diversi progetti innovativi nel campo della protezione delle infrastrutture critiche dalle minacce informatiche e fisiche e a rendere le città più intelligenti e sicure.[7]
- L'UE ha pubblicato un invito a presentare proposte, del valore di 10,5 milioni di euro, per progetti nell'ambito della cibersicurezza. La Commissione ha lanciato un nuovo invito a presentare proposte del valore di 10,5 milioni di euro attraverso il meccanismo per collegare l'Europa (MCE) per progetti finalizzati a rafforzare le capacità di cibersicurezza dell'Europa e la cooperazione tra gli Stati membri.[8]

Ricerca e innovazione nella CTI

Diffusione rapida di metodi e contenuti in materia di CTI

Durante il periodo in esame sono state individuate diverse esigenze di ricerca e in questa sede vengono proposte le azioni per affrontarle, raggruppate in alcune categorie per rispecchiare meglio il campo di applicazione. Benché non esenti da sovrapposizioni, queste categorie sono indicative delle aree di potenziale miglioramento della CTI.

- **I risultati dei progetti di ricerca nell'area della CTI devono essere valutati e mappati in un contesto di CTI più ampio** al fine di individuare sovrapposizioni e lacune e di renderli confrontabili con i prodotti, i servizi e le prassi di CTI commerciali esistenti. Ciò favorirà la diffusione dei risultati alla comunità di utenti. Allo stesso tempo, le lacune esistenti verranno colmate da funzioni, contenuti e processi supplementari. I progetti dell'UE (Orizzonte 2020) attinenti alla CTI sono candidati eccellenti per questo compito, contribuendo a migliorare le pratiche di CTI.
- **Dovranno essere promossi la fornitura e l'impiego di materiale open source sulla CTI**, allo scopo di facilitare il trasferimento delle conoscenze ma anche di abbassare la soglia delle competenze di CTI. Open-CTI è il candidato perfetto per questo scopo, in quanto supporta l'ingestione di CTI proveniente da più fonti in un'unica base che può essere condivisa tra vari utenti, offrendo nel contempo una serie di funzioni per la gestione di tali informazioni. Adottando Open-CTI, gli utenti saranno in grado di ottenere informazioni preziose a una soglia di competenza relativamente bassa.

_Ricerca che produce tendenze emergenti

La necessità di **rafforzare la CTI** con altri strumenti di cibersicurezza consolidati richiede l'evoluzione strutturale e contestuale di questo settore. Allo stesso tempo, i progressi tecnologici determinati dalle tecnologie emergenti pongono la questione di come la CTI possa beneficiare di questi sviluppi. Pertanto, le esigenze della **potenziale ricerca** nel campo della CTI contribuiranno a migliorare i processi, le funzioni, l'automazione, la struttura e la convalida dei contenuti, la fornitura di servizi, la speed-to-user/diffusione, l'implementazione e le mappature della CTI.

La CTI si è saldamente affermata nel campo della cibersicurezza come strumento essenziale per migliorare l'agilità e l'efficienza nella difesa dagli attacchi informatici.

Ricerca e innovazione nella CTI

Funzionalità, livello di automazione e conformità ai requisiti di maturità

- **L'automazione dei processi assumerà un ruolo essenziale nella CTI**. Sebbene i moderni attacchi informatici siano diventati fortemente automatizzati, le organizzazioni tentano di difendersi manualmente o con un utilizzo parziale dell'automazione. Si tratta di una lotta impari, che rallenta la velocità e la capacità di risposta. Studiare la potenziale automazione dei processi di CTI sarà fondamentale per trovare un equilibrio tra aggressori e difensori. Il raggiungimento di questo obiettivo richiederà un'analisi approfondita delle fasi dei processi di CTI e delle opzioni per automatizzare queste fasi grazie alle tecnologie disponibili ed emergenti.
- **I requisiti di maturità della CTI dovranno essere identificati in maggiore dettaglio**. Nonostante siano stati elaborati alcuni criteri e requisiti per la scelta delle funzioni di CTI (ad esempio piattaforme di Threat Intelligence o TIP) per vari profili di utente, requisiti analoghi saranno necessari per ulteriori prodotti, servizi e strumenti di CTI. Tali requisiti saranno associati a diversi livelli di maturità degli utenti, spesa e tipologie di CTI. Criteri e requisiti analoghi sono necessari per vari altri elementi di un'infrastruttura di CTI, come strumenti, buone pratiche, piattaforme di condivisione, ecc. Pertanto, oltre allo sviluppo di modelli di maturità delle capacità di CTI, è necessaria la ricerca per mostrare come le funzioni di CTI corrispondono ai vari livelli di maturità della CTI stessa. Questo lavoro contribuirà a velocizzare l'adozione delle pratiche di CTI.
- **L'uso dell'intelligenza artificiale/apprendimento automatico nella CTI merita un approfondimento**. Consentirà di ridurre il numero di operazioni manuali nella CTI e di aumentare il valore delle funzioni di apprendimento automatico all'interno delle attività di CTI.

Costruire ponti verso le aree correlate

- È necessario sviluppare **approcci nuovi per l'ingestione di conoscenza in materia di CTI da parte dei domini** che possono trarne vantaggio. Alcuni esempi sono i poligoni virtuali, le minacce ibride, le catene di fornitura e le valutazioni e crisi geopolitiche. Le domande da porsi a tale riguardo sono: Quali sono i punti in cui la CTI può essere presa in considerazione? Quali sono i contenuti di CTI pertinenti? Quali sono i criteri di convalida per l'adeguatezza delle informazioni di CTI? Come è possibile «agganciare» la CTI alle informazioni sul dominio interessato? Quali tipi di informazioni derivanti da questi domini possono essere aggiunti alla CTI? Le sinergie che si riflettono in tali domande possono incrementare i casi d'uso e migliorare la qualità dei contenuti in modo omnidirezionale.

- **La CTI è essenziale per una serie di discipline.** Gli esempi includono la valutazione/gestione del rischio e la definizione dei requisiti di protezione e della certificazione. Sarà un vantaggio per queste discipline utilizzare la CTI nel modo corretto. È possibile individuare il contributo della CTI a queste discipline utilizzando informazioni quali modelli di minacce, informazioni sugli attori delle minacce (capacità, moventi), metodi di attacco ed exploit. Sebbene esista del materiale pertinente (ad esempio il framework di attacco ATT&CK[8]), è necessario un lavoro significativo per identificare e standardizzare tali interfacce informative.

Ricerca e innovazione nella CTI

Efficacia delle attività di CTI

- **I metodi per un utilizzo efficace della CTI costituiranno uno strumento per il processo decisionale.** Tali metodi di impiego efficiente della CTI aiuteranno i decisori a comprendere il valore della CTI e gli operatori a valutarne il ritorno sull'investimento. I metodi/KPI dovranno prendere in considerazione fattori che vanno al di là del contenuto della CTI, tenendo conto dei miglioramenti realizzati nell'intero ciclo di vita della gestione della sicurezza e della mitigazione del rischio. In via ottimale, la misurazione dell'efficacia dell'investimento nella CTI farà parte di una considerazione molto più ampia dell'economia della cibersicurezza in vari tipi di organizzazioni (ad esempio secondo i requisiti di sicurezza, i livelli di maturità, ecc.).

- A dispetto della prevalenza di strumenti a basso costo per l'aggregazione, l'analisi e la diffusione della CTI, **può essere necessario condurre ricerche per trovare strumenti automatizzati per la gestione della CTI** fruita e prodotta. Oltre ai formati di dati standardizzati (ad esempio file CSV, STIX, TAXII), le funzioni di CTI standard possono essere oggetto di tali ricerche, seguite dallo sviluppo di strumenti open source a basso costo a supporto di dette funzioni.

Evoluzione della struttura e del contenuto della CTI

- Parallelamente alla penetrazione della CTI in ulteriori ambiti, **sarà necessario che le informazioni provenienti da questi contesti vengano reinviate alla base di conoscenza originale della CTI**. Ad esempio, devono essere definite strutture di CTI per acquisire informazioni geopolitiche e sulle minacce ibride. Lo stesso vale per la rilevanza delle CTI per rischi, incidenti, analisi forensi, livelli di affidabilità, ecc. I formati di CTI esistenti dovranno evolversi per acquisire le informazioni scaturite da queste dipendenze nella CTI.

- **Le tecnologie emergenti come l'IA** possono essere utilizzate per convalidare la CTI analizzata. Tali strumenti possono potenziare o addirittura sostituire l'analisi della CTI manuale, ma anche fornire un supporto per tutto il ciclo di vita della CTI (ad esempio verificarne la pertinenza in base alle informazioni sugli incidenti esistenti). Questi nuovi approcci alla CTI miglioreranno la qualità e la pertinenza delle informazioni.

Riferimenti bibliografici

1. Il concetto di poligono virtuale è stato inizialmente definito nel 2013 dall'Agenzia europea per la difesa (AED) nel rapporto «Common Staff target for military cooperation on cyber ranges in the European Union» (obiettivo comune in materia di personale per la collaborazione militare sui poligoni virtuali nell'Unione europea), come ambiente polivalente a sostegno di tre processi primari: sviluppo, garanzia e diffusione delle conoscenze.

2. «ENISA Threat Landscape for 5G Networks». 21 novembre 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

3. https://www.concordia-h2020.eu/

4. https://echonetwork.eu/

5. https://www.sparta.eu/news/

6. https://cybersec4europe.eu/

7. https://ec.europa.eu/programmes/horizon2020/en/news/eu-grants-%E2%82%AC38-million-protection-critical-infrastructure-against-cyber-threats

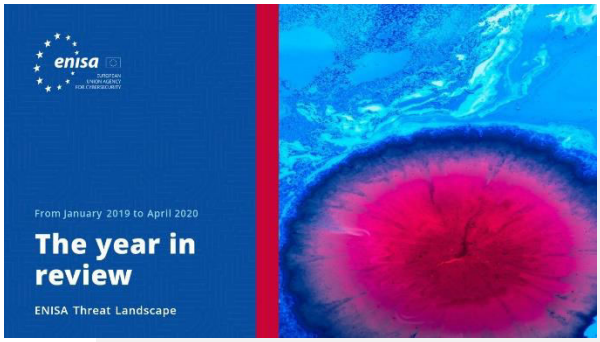
8. https://ec.europa.eu/digital-single-market/en/news/eu105-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and

9. https://attack.mitre.org/

«La CTI si è saldamente affermata nel campo della cibersicurezza come strumento essenziale per migliorare l'agilità e l'efficienza nella difesa dagli attacchi informatici».

in ETL 2020

Correlati



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

Una sintesi delle principali tendenze della sicurezza informatica dell'anno.

LEGGI LA RELAZIONE

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

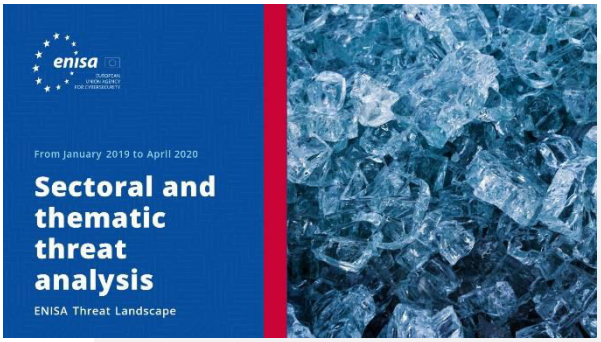
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Incidenti principali nell'UE e a livello mondiale**

Principali incidenti di cibersicurezza verificatisi tra gennaio 2019 e aprile 2020.

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

Roadmap on the Cooperation Between CSIRTS and LE (Tabella di marcia sulla cooperazione tra CSIRTS e autorità di contrasto)

Una tabella di marcia sulla cooperazione tra i CSIRT, in particolare con le autorità di contrasto nazionali e governative e il potere giudiziario.

LEGGI LA RELAZIONE

EU MS Incident Response Development Status Report (Relazione sullo stato dello sviluppo della risposta agli incidenti negli Stati membri dell'UE)

Uno studio finalizzato ad analizzare l'attuale assetto operativo di risposta agli incidenti all'interno dei settori previsti nella direttiva NIS e a individuare i cambiamenti recenti.

LEGGI LA RELAZIONE

ENSIA CSIRT maturity assessment model (Modello ENISA di valutazione della maturità dei CSIRT)

Versione aggiornata di «Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity» (Sfide per i CSIRT nazionali in Europa nel 2016: studio sulla maturità dei CSIRT), pubblicato dall'ENISA nel 2017

LEGGI LA RELAZIONE

«La complessità delle competenze in materia di minacce è aumentata nel 2019, con molti avversari che utilizzano exploit, furto di credenziali e attacchi a più livelli».

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