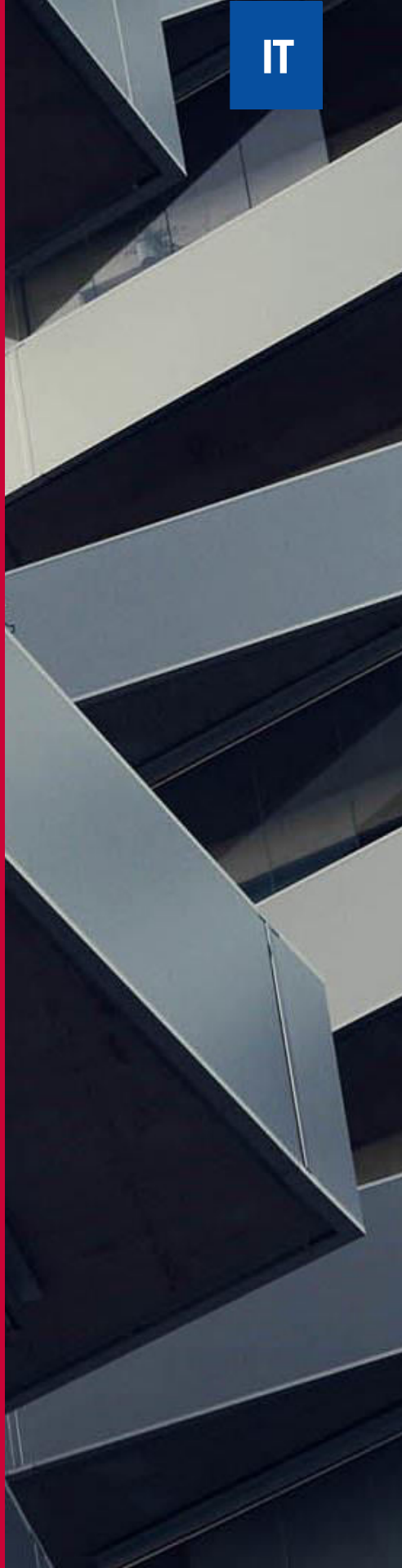
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT



Da gennaio 2019 ad aprile 2020

Violazione dei dati

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Una violazione dei dati è un tipo di incidente di cibersicurezza caratterizzato dall'accesso a informazioni (o a parte di un sistema informativo) senza la giusta autorizzazione, in genere con intento doloso, che ha come conseguenza la potenziale perdita o il potenziale uso improprio di tali informazioni. Comprende anche l'«errore umano» che spesso si verifica durante la configurazione e l'implementazione di determinati servizi e sistemi e può comportare un'esposizione involontaria dei dati.[1]

In molti casi, le aziende o le organizzazioni non sono consapevoli di una violazione dei dati che si verifica nel loro ambiente, a causa della sofisticatezza dell'attacco e talvolta della mancanza di visibilità e di classificazione nel loro sistema informativo.[2] Secondo le ricerche, occorrono circa 206 giorni per identificare una violazione dei dati in un'organizzazione.[3] Pertanto, il tempo necessario per contenere, riparare e recuperare i dati significa tempi più lunghi per il ritorno alla normalità.

Nonostante tutti i rischi in gioco, le organizzazioni conservano un numero ancora maggiore di dati[4] utilizzando infrastrutture di archiviazione sul cloud e in ambienti in locale complessi. Questi ambienti sono via via esposti a rischi nuovi e diversi in proporzione alla sensibilità delle informazioni memorizzate. Non sorprende quindi che il numero di violazioni dei dati sia aumentato nel 2019 e nel 2020. Nuove evidenze suggeriscono inoltre che l'impatto non viene percepito solo quando la violazione dei dati viene scoperta, ma a livello finanziario l'effetto può permanere per più di due anni dall'incidente iniziale.

Risultati

54%_di aumento nel numero totale di violazioni a metà del 2019, rispetto al 2018.

Il 71%_ delle violazioni dei dati aveva un movente economico. Circa il 25% aveva obiettivi strategici a lungo termine (Stato nazione/spionaggio).[5]

Il 32%_delle violazioni dei dati implica attività di phishing, secondo la IOCTA 2019.[6] Un rapporto suggerisce che il phishing è in cima alla lista delle principali cause di violazione dei dati. Il rapporto indica inoltre che l'e-mail è il principale metodo di consegna del malware (94%) in una catena di eventi che porta a una violazione dei dati.[3]

Il 52%_delle violazioni dei dati ha implicato un'attività di hacking.[5] Altre tattiche impiegate sono attacchi di ingegneria sociale (33%), malware (28%) ed errori (21%). Dal 2016 l'hacking è la causa principale delle violazioni dei dati nel settore sanitario. Nel corso del 2019 quasi il 59% delle violazioni segnalate era imputabile ad attività di hacking.[7]

Il 70%_delle violazioni dei dati comporta la divulgazione di e-mail. Sebbene il nome utente/l'e-mail e le password (cioè le credenziali) siano facilmente modificabili, al contrario dei dati personali (cioè la data di nascita), nelle violazioni dei dati l'attenzione si concentra soprattutto su tali elementi.[8]

Il 55%degli intervistati di un'indagine Eurobarometro ha risposto di temere un accesso ai loro dati da parte di criminali e truffatori.

Sequenza temporale

2019

_ Gennaio

MEGA cloud (NZ) ha subito una violazione dei dati che ha provocato la divulgazione di 770 milioni di e-mail e 21 milioni di password.[9]

_ Febbraio

620 milioni di account rubati da 16 siti web compromessi ora in vendita sul dark web, afferma fiero il venditore.[10]

_ Marzo

12,5 milioni di cartelle cliniche di donne in gravidanza di un centro sanitario pubblico indiano (IN), risalenti al 2014, sono state rivelate al pubblico.[11]

_ Agosto

Importante violazione rilevata nel sistema biometrico utilizzato dalle banche, dalla polizia (britannica) e dalle imprese nel settore della difesa.[16]

_ Settembre

Mastercard (BE) ha subito una violazione dei dati che ha interessato circa 90 000 clienti in Europa.[17]

_ Ottobre

I dati degli account di oltre 7,5 milioni di utenti di Adobe (USA) sono stati rivelati a causa di una banca dati online non protetta.[18]

_ Novembre

UniCredit (IT) vittima di una violazione dei dati, con esposizione di 3 milioni di record.[19]

_ Dicembre

Il fornitore di telecamere intelligenti Wyze (USA) ha subito due violazioni alla fine di dicembre, quando i database sono rimasti esposti per oltre due settimane.[20]

2020

_ Gennaio

Sono stati violati 250 milioni di record di assistenza e supporto clienti di Microsoft (USA), risalendo fino al 2005.[21]

_ Aprile

Facebook (USA) ha denunciato una violazione dei dati che ha rivelato 540 milioni di record di utenti su server esposti.[12]

_ Maggio

Resi pubblici centinaia di milioni di dati di polizze sui rischi legali delle compravendite (title insurance) della First American Financial Corp. (USA)[13]

_ Luglio

Violati i dati personali dei clienti di carte di credito di Capital One (USA).[15]

_ Giugno

100 milioni di record esposti in seguito all'accesso non autorizzato ai dati memorizzati di clienti Evite.[14]

_ Febbraio

Server cloud di Google (USA) non protetto contenente i dati personali di 200 milioni di residenti statunitensi.[22]

_ Marzo

La società di soluzioni biometriche Antheus Tecnologia (BR) è stata oggetto di una fuga di dati.[23]

_ Aprile

Hacker hanno ottenuto i dati di accesso di due dipendenti di Marriott (USA) e si sono introdotti nel sistema nel gennaio 2020.[24]

Tendenze

_Il costo di una violazione dei dati per le organizzazioni si ripartisce su molti anni

I ricercatori nel campo della sicurezza hanno riscontrato che un terzo dei costi legati a una violazione dei dati viene sostenuto dopo più di un anno dall'incidente. Per la precisione, circa il 22% di questi costi è sostenuto nel secondo anno, mentre l'11% oltre 2 anni dopo l'incidente iniziale. Questi tassi sono risultati più elevati per le organizzazioni altamente regolamentate, come quelle dei servizi finanziari e della sanità, rispetto ad altri settori.[3]
L'adozione di ambienti cloud o multi-cloud sta aumentando con rapidità, analogamente alla quantità di dati memorizzati ed elaborati in tali ambienti.

_Piccoli errori potrebbero portare a grandi violazioni

Proteggere l'ambiente cloud senza sacrificare tutta la flessibilità che esso offre per l'infrastruttura e le risorse può essere problematico. Un unico errore di configurazione può comportare l'esposizione dell'intero database sensibile. Un ricercatore della sicurezza ritiene che la maggior parte delle violazioni dei dati nel cloud sia conseguenza di un'errata configurazione e che sia per lo più involontaria. Netflix, Ford e TD Bank sono solo alcuni esempi. Da un punto di vista diverso, sebbene le violazioni dei dati derivanti da tentativi malevoli continuino a risultare più onerose, quelle causate da malfunzionamenti dei sistemi o da errori umani rappresentano ancora un costo considerevole, pari in media a 3,24 milioni di dollari USA (circa 2,74 milioni di euro).[3]

Le violazioni dei dati sono più onerose per le piccole imprese

Il costo delle violazioni dei dati per le imprese o le grandi organizzazioni con più di 25 000 dipendenti è di 204 dollari USA (circa 173 EUR) per dipendente, per un importo totale stimato intorno a 5,11 milioni di dollari USA (circa 4,33 milioni di EUR). Per le piccole imprese (500-1 000 dipendenti) il costo medio si aggira invece sui 3 533 dollari USA (circa 3 000 EUR) per dipendente, che rappresenta un costo totale di 2,65 milioni di dollari USA (circa 2,24 milioni di EUR).[3]

Il guadagno economico è la motivazione principale

È noto che dietro le violazioni dei dati vi sono attori malintenzionati (tenendo comunque presente che a volte le violazioni possono essere il risultato di un errore). In tal senso, gli attori delle minacce esterne sono la causa principale delle violazioni dei dati, e questo potrebbe includere attività come le botnet[4]. Al riguardo, il guadagno economico è stato ripetutamente identificato come motivazione principale delle violazioni dei dati promosse da questi gruppi di attori. Anche lo spionaggio[4] è stato uno dei moventi fondamentali delle violazioni dei dati, ma non in cima alla classifica al pari del guadagno personale o economico. Tale tendenza è risultata pressoché coerente con i risultati osservati nel periodo 2010-2011.[5]

Tendenze

Informatica quantistica e timori per la sicurezza dei dati

I requisiti della crittografia rivestono un ruolo vitale nell'era dell'informatica quantistica e mettono in luce problemi critici di sicurezza. Il 72% delle organizzazioni ritiene che l'informatica quantistica influenzerà strategicamente le loro attività relative alla crittografia (nei prossimi 5 anni). Secondo i risultati dell'indagine, il 92% degli intervistati è preoccupato per l'esposizione di dati sensibili legata all'uso di questa tecnologia nell'industria informatica. Le principali strategie suggerite dagli intervistati per affrontare tali timori sono state la modifica dell'architettura di sicurezza e l'implementazione di infrastrutture di gestione delle chiavi.[26]

Assistenza sanitaria: un bersaglio costante per gli attori malintenzionati

L'assistenza sanitaria continua a essere uno degli obiettivi più interessanti per i criminali informatici che sfruttano tecniche di ransomware[7] e phishing[7] che costano alle organizzazioni di tale settore milioni di euro per il contenimento dell'impatto e il successivo recupero. Nel 2019, 400 aziende sanitarie hanno segnalato una violazione dei dati nelle cartelle cliniche dei pazienti: una cifra record per le organizzazioni di questo settore.[7]

Multi-cloud: la nuova sfida per la sicurezza dei dati

Un'indagine condotta da un ricercatore della sicurezza ha riferito che 9 aziende su 10 intendono utilizzare o stanno già utilizzando ambienti cloud. Circa il 44% degli intervistati ritiene inoltre che questi ambienti costituiscano una sfida in termini di attuazione di misure di sicurezza dei dati adeguate.[25]

Tipi di dati esposti (%)

Tipo di dati	2019	2018	2017
E-mail	70	44	32
Password	64	39	27
Nome	23	37	41
Varie	18	19	15
Numero di sicurezza sociale	11	22	27
Carta di credito	11	16	19
Indirizzo	11	22	30
Conto	10	7	4
Non noto	8	13	18
Data di nascita	8	13	12
Medici	5	9	7
Finanziari	5	13	19

Tabella 1 - Fonte: Cyber Risk Analytics[8]

Tendenze

_Continuo calo delle violazioni in ambiente «card-present»

Secondo un rapporto sulla sicurezza, nel corso del 2019 si è rilevata una diminuzione delle violazioni presso i punti vendita e di skimming delle carte di credito (con utilizzo della carta fisica). Ciò rappresenta un passaggio dal tradizionale skimming agli sportelli automatici[7] e dai pagamenti con carta all'applicazione web nel settore del commercio al dettaglio. Benché il numero di incidenti in questo ambito sia calato, non sarebbe esatto concludere che vi sia una riduzione del numero di violazioni dei dati; si tratta piuttosto di un cambiamento di vettore. Il calo potrebbe essere tuttavia correlato a una più diffusa adozione di carte/terminali con chip e PIN (noti anche come EMV).[6]

_Che cosa aspettarsi nel prossimo futuro?

Secondo un ricercatore della sicurezza, le organizzazioni sanitarie dovrebbero prepararsi a un aumento del 10%-15% del numero di violazioni dei dati, in cui il principale bersaglio sarà costituito dai loro fornitori di servizi[7]. A livello più generale, sulla base dei risultati dei primi 6 mesi del 2019, si prevede un aumento del numero di violazioni dei dati a un ritmo allarmante, nonostante la consapevolezza dei dirigenti e gli sforzi compiuti da molte organizzazioni per proteggere i loro dati.[8]

_Violazioni dei dati per settore e dimensioni dell'organizzazione

Incidenti	Violazioni	Piccole	Grandi	Non note
Alloggio	61	34	7	20
Amministrativo	17	6	6	5
Agricoltura	2	2	0	0
Edilizia	11	7	3	1
Istruzione	99	14	8	77
Intrattenimento	10	2	3	5
Finanza	207	26	19	162
Assistenza sanitaria	304	29	25	250
Informazioni	155	20	18	117
Direzione	2	1	1	0
Produzione	87	10	22	55
Attività mineraria	15	2	5	8
Altri servizi	54	6	5	43
Professionale	157	34	10	113
Pubblico	**330**	**17**	**83**	**230**
Immobiliare	14	6	3	5
Vendita al dettaglio	139	46	19	74
Commercio	16	4	8	4
Trasporto	36	3	9	24
Servizi pubblici	8	2	0	6
Non noto	289	0	109	180
Totale	2 013	271	363	1 379

Tabella 2 - Fonte: Verizon DBIR, 2019[5]

Vettori di attacco

- **E-MAIL/PHISHING.** Impersonare un fornitore o un partner terzo utilizzando la posta elettronica è una tattica efficace per gli attori malintenzionati. Si tratta notoriamente del vettore più spesso utilizzato dai criminali informatici per colpire le loro vittime, nonché della causa della maggior parte delle violazioni dei dati (quasi il 40% delle violazioni in ambito sanitario).[1]
- **CLOUD/APPLICAZIONI WEB.** Riguarda l'uso di applicazioni web come vettore per i tentativi di violazione dei dati o di attività critiche da parte di attori malintenzionati. Il furto di credenziali per accedere a portali di posta elettronica basati sul web è un esempio tipico. Lo sfruttamento dei punti deboli nei server applicativi per iniettare/veicolare malware per il furto di informazioni o attacchi di formjacking sono altri esempi relativi a questo vettore.[2]
- **MINACCE INTERNE.** Si riferiscono principalmente a tentativi non autorizzati o dolosi di utilizzare risorse. Va notato che, in linea generale, nell'analisi e nel reporting, anche per l'errata configurazione o gli errori (errore umano) da parte dei team aziendali si può parlare di «minacce interne». Anche se la maggior parte delle violazioni dei dati è promossa da attori esterni malintenzionati, resta comunque il fatto che gli insider con o senza accesso privilegiato svolgono un ruolo chiave in tali violazioni.[5]

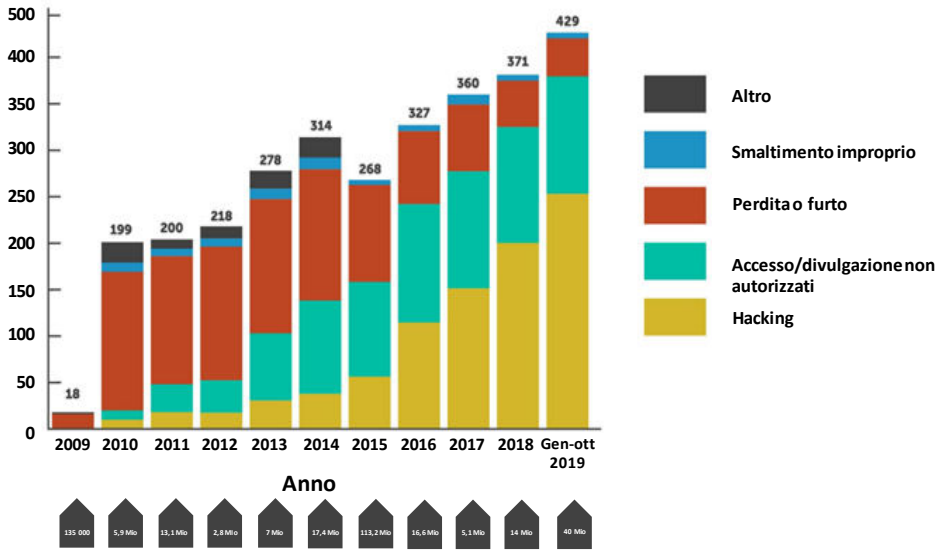
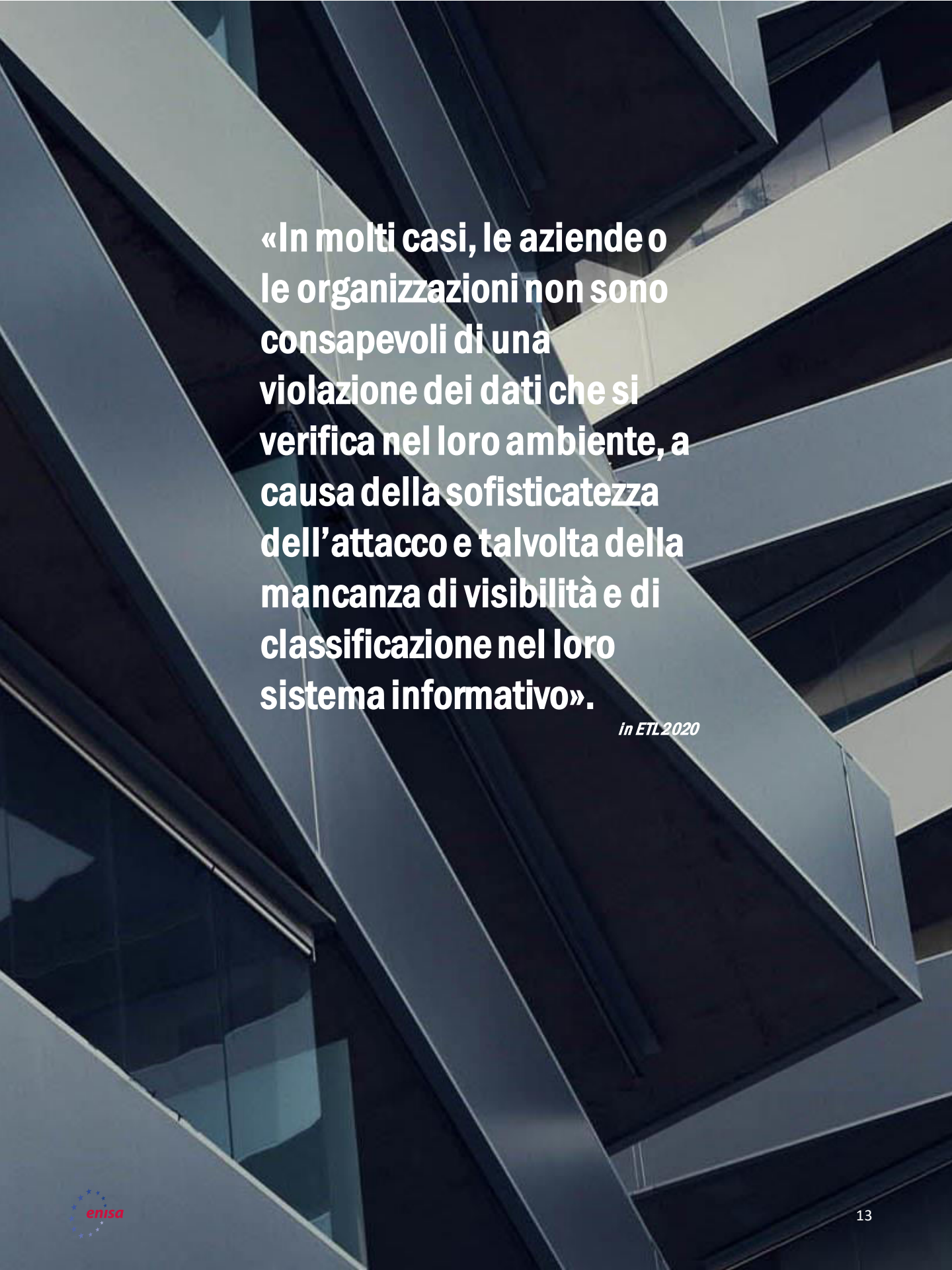


Figura 1. Entità coinvolte in una violazione. Fonte: Horizon[1]



«In molti casi, le aziende o le organizzazioni non sono consapevoli di una violazione dei dati che si verifica nel loro ambiente, a causa della sofisticatezza dell'attacco e talvolta della mancanza di visibilità e di classificazione nel loro sistema informativo».

in ETL 2020

Mitigazione

Azioni proposte

- La violazione dei dati è in genere la conseguenza di altre minacce e la mitigazione è sovrapponibile ad altre discusse in questa relazione.
- Considerare l'investimento in strumenti di sicurezza dei dati ibridi, incentrati sul funzionamento in un modello di responsabilità condivisa per gli ambienti basati sul cloud.[26]
- Elaborare e mantenere un piano di sensibilizzazione alla cibersicurezza. Prevedere scenari di formazione e simulazione per identificare le campagne di ingegneria sociale e di phishing per il personale.[7]
- Costituire e mantenere un team di risposta agli incidenti e valutare di frequente i piani di risposta agli incidenti.[3]
- Identificare e classificare i dati sensibili/personali e applicare misure per la crittografia di tali dati in transito e a riposo.[3] In altre parole, implementare funzionalità di prevenzione della perdita di dati.
- Aumentare gli investimenti in strumenti di rilevamento e di allerta e nella capacità di contenere una violazione dei dati e di rispondere alla stessa.
- Sviluppare e mantenere solide politiche di applicazione di password forti (gestione delle password) e dell'uso dell'autenticazione a più fattori.
- Considerare l'utilizzo di modelli che adottino il principio del «privilegio minimo» per la sicurezza delle risorse sia in locale sia in remoto (ossia modelli «zero trust»).
- Investire nella creazione di politiche e piani per interagire con i team di governance, gestione del rischio e conformità.[26]


«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

Riferimenti bibliografici

1. «What is data breach?» Norton. https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

2. «What is data breach?» Malwarebytes. https://www.malwarebytes.com/data-breach/

3. «Cost of Data Breach Report.» 2019. IBM Security, Ponemon Institute. https://www.ibm.com/security/data-breach

4. Dhritimaan Shukla, Kush Wadhwa. «Data breach – threat landscape. Unauthorised exposure of an organisation's critical data.» PWC India. https://www.pwc.in/consulting/forensic-services/data-breach-threat-landscape.html

5. «Verizon Data Breach Investigations Report.» 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

6. Catherine De Bolle. «Internet Organised Crime Threat Assessment (IOCTA).» 2019. Centro europeo per la lotta alla criminalità informatica (EC3), Europol. https://www.europol.europa.eu/iocta-report

7. «2020 Healthcare Cybersecurity Horizon Report.» 2020. Fortified Health Security. https://fortifiedhealthsecurity.com/wp-content/uploads/2019/12/Fortified-Health-Security-2020-Horizon-Report.pdf

8. Inga Goddijn. «2019 Midyear QuickView Data Breach Report – Cyber Risk Analytics.» Agosto 2019. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf

9. Troy Hunt. «The 773 Million Record "Collection #1" Data Breach.» 17 gennaio 2019. TroyHunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

10. Chris Williams. «620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts.» 11 febbraio 2019. The Register. https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

11. Catalin Cimpanu. «Indian govt agency left details of millions of pregnant women exposed online.» 1º aprile 2019. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

12. «Losing Face: Two More Cases of Third-Party Facebook App Data Exposure.» 3 aprile 2019. UpGuard. https://www.upguard.com/breaches/facebook-user-data-leak

13. «First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records.» 24 maggio 2019. KrebsonSecurity. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

14. «Data Incident, Evite.» 14 maggio 2019. Evite. https://www.evite.com/security/update

15. «Information on the Capital One Cyber Incident.» 23 settembre 2019. CapitalOne. https://www.capitalone.com/facts2019/

16. Josh Taylor. «Major breach found in biometrics system used by banks, UK police and defence firms.» 14 agosto 2019. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

17. Neil Hodge. «Mastercard reveals data breaches in third-party loyalty program.» 27 agosto 2019. Compliance Week. https://www.complianceweek.com/data-privacy/mastercard-reveals-data-breaches-in-third-party-loyalty-program/27614.article

18. Catalin Cimpanu. «Adobe left 7.5 million Creative Cloud user records exposed online.» 26 ottobre 2019. ZDNet. https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/

19. Charlie Osborne. «UniCredit reveals data breach exposing 3 million customer records.» 28 ottobre 2019. ZDNet. https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/

20. Chris Isidore. «Smart camera maker Wyze hit with customer data breach.» 30 dicembre 2019. CNN. https://edition.cnn.com/2019/12/30/tech/wyze-data-breach/index.html

21. Davey Winder. «Microsoft Security Shocker As 250 Million Customer Records Exposed Online.» 22 gennaio 2020. Forbes. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#2d3f9dca4d1b

22. Paul Bischoff. «US property and demographic database of 200 million records leaked on the web.» 5 marzo 2020. comparitech. https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/

23. Jim Wilson. «Brazil: Millions of Records Leaked, Including Biometric Data.» 11 marzo 2020. Safety Detectives. https://www.safetydetectives.com/blog/antheus-leak-report/

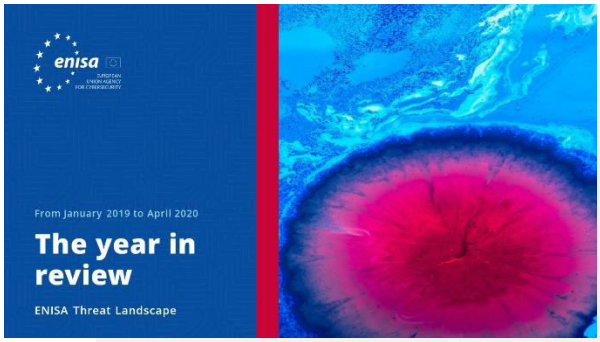
24. Zack Whittaker. «Marriot says 5.2 million guest records were stolen in another data breach.» 1° aprile 2020. Techrunch. https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?renderMode=ie11

25. «2019 Thales Data Threat Report – Global Edition» Thales Security, 2019. https://cpl.thalesgroup.com/data-threat-report

26. «2020 Thales Data Threat Report – Global Edition» Thales Security, 2020. https://cpl.thalesgroup.com/data-threat-report

27. Laura Paine. «2019 Verizon DBIR Shows Web Applications and Human Error as Top Sources of Breach.» 8 maggio 2019. Veracode. https://www.veracode.com/blog/security-news/2019-verizon-dbir-shows-web-applications-and-human-error-top-sources-breach

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

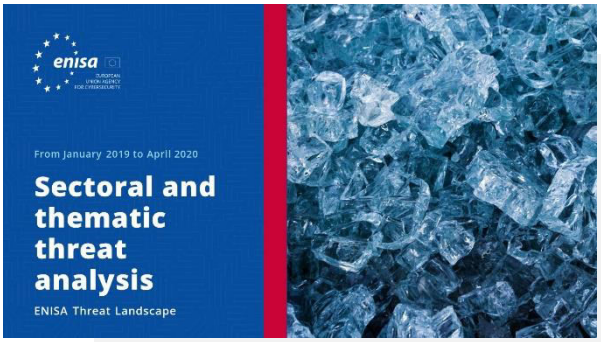
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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



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.

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

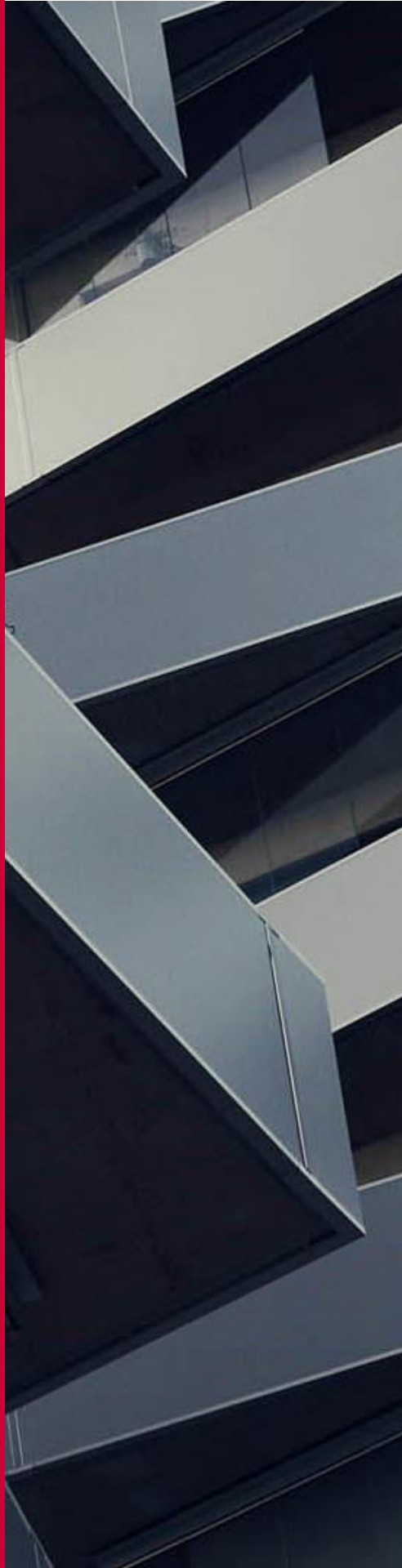
Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013.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