enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Fuga di informazioni

Panorama delle minacce

Quadro generale

Si verifica una violazione dei dati quando i dati di cui un'organizzazione è responsabile subiscono un incidente di sicurezza con conseguente violazione della riservatezza, della disponibilità o dell'integrità.[1] Una violazione dei dati causa spesso una fuga di informazioni, che rappresenta una delle principali minacce informatiche, con impatto su un'ampia varietà di informazioni compromesse, dalle informazioni di identificazione personale (Personal Identifiable Information, PII), ai dati finanziari memorizzati nelle infrastrutture IT fino ai dati sanitari personali (Personal Health Information, PHI) conservati negli archivi dei prestatori di servizi sanitari.

Quando ci si imbatte in violazioni della sicurezza nei titoli di bollettini, blog, giornali e rapporti tecnici, l'attenzione si concentra soprattutto sugli avversari o sul catastrofico fallimento dei processi e delle tecniche di ciberdifesa. Tuttavia la verità indiscutibile è che, nonostante l'impatto o la portata di un tale evento, la violazione è in genere causata un'azione individuale o da un fallimento dei processi dell'organizzazione.[2]

Risultati

2 013_divulgazioni dei dati confermate nel 2019

Nel primo semestre del 2019 le organizzazioni hanno riscontrato un aumento dell'11% delle divulgazioni, in confronto al 2018.[5, 6]

Il 14%_di tutti gli incidenti nel settore finanziario era costituito da divulgazioni di dati

Nel 47% dei casi la vittima era una banca.[9]

4,1_miliardi di record di dati sono stati divulgati a livello globale nel primo semestre del 2019

E-mail e password erano in cima alla lista.[10]

5,46_milioni di euro è il costo massimo sostenuto dal settore sanitario[11]

Kill chain

Fuga di informazioni

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.

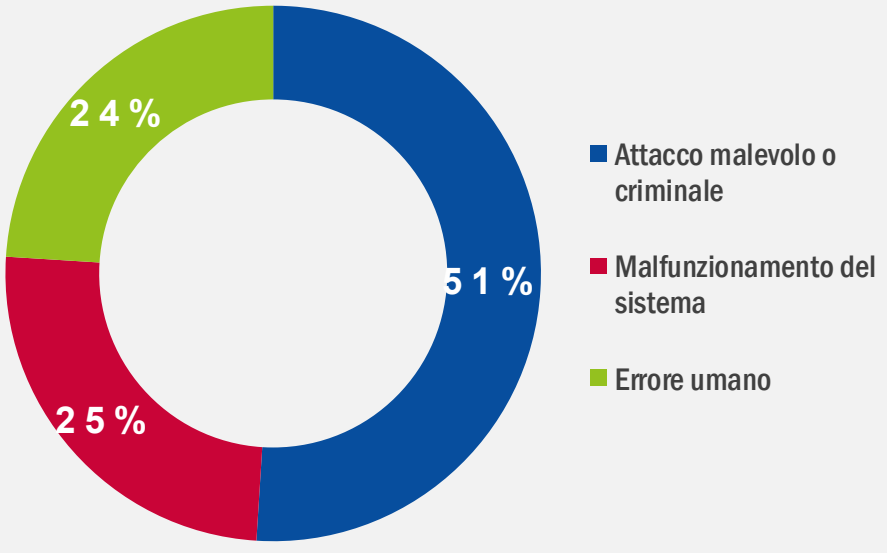
MAGGIORI INFORMAZIONI

Incidenti

I principali incidenti di fuga di dati

- Nel gennaio 2019 il ricercatore indipendente Troy Hunt ha scoperto 773 milioni di indirizzi e-mail e password di utenti nel **servizio di archiviazione cloud MEGA**. Hunt ha denominato questo set di dati violato «Collection#1» e ha informato il servizio «Have I been Pwned?» in modo da avvisare i proprietari degli account di modificare le loro password per accedere alla piattaforma MEGA.[12] Nello stesso mese alcuni malviventi hanno divulgato dati personali, comunicazioni private e informazioni finanziarie di centinaia di **politici tedeschi**, prendendo di mira esponenti di tutti i partiti, tranne l'estrema destra AfD (Alternative für Deutschland).[6]
- Nel febbraio 2019 più di 61 milioni di account sono stati raccolti da 16 siti web e messi in vendita sul dark web. I proprietari dei siti Whitepages, Dubsmash, Armor Games, 500px e ShareThis hanno visto i dati rubati dei loro utenti in vendita a meno di 20 000 dollari USA (circa 17 000 euro) in bitcoin.[13]
- Nel marzo 2019 le credenziali di centinaia di milioni di utenti di **Facebook** e **Instagram** sono state divulgate a causa della scadente gestione delle password memorizzate da parte della società di social media.[14]
- Nell'aprile 2019, in India 12,5 milioni e mezzo di cartelle cliniche di donne in gravidanza sono state divulgate, a causa della fuga di dati da un server appartenente a un'agenzia sanitaria pubblica. Le informazioni mediche rivelate erano collegate alla legge indiana sulle tecniche diagnostiche preconcezionali e prenatali, che vietava la determinazione del sesso prenatale nel tentativo di impedire alle famiglie indiane di abortire qualora il nascituro sia di sesso femminile e di distorcere il rapporto dei sessi alla nascita verso i maschi.[15]

- Nel maggio 2019 **DoorDash**, un servizio di consegna di cibo a domicilio, ha subito una violazione dei dati che ha interessato quasi 5 milioni di utenti. L'indagine successiva ha stabilito che l'accesso ha riguardato informazioni quali nomi, indirizzi e-mail, indirizzi di consegna, cronologia degli ordini, numeri di telefono e password. L'azienda ha dichiarato che gli aggressori hanno avuto accesso anche alle ultime quattro cifre delle carte di credito e dei numeri di conto corrente di alcuni consumatori.[16]
- Nel giugno 2019 l'**American Medical Collection Agency (AMCA)** ha iniziato a informare i clienti di un'intrusione abusiva nel sistema che ha violato i dati medici e di fatturazione e i dati di alcuni di loro, tra cui 11,9 milioni di record di **Quest Diagnostics**, una delle più grandi società di analisi del sangue negli Stati Uniti. Secondo una recente dichiarazione (modello 8-K) presentata alla Securities and Exchange Commission, un hacker ha avuto accesso al sistema dell'AMCA per quasi otto mesi tra il 1° agosto 2018 e il 30 marzo 2019.[17]



Cause profonde della divulgazione di informazioni. Fonte: Ponemon, IBM Security[22]

Incidenti

I principali incidenti di fuga di dati

- Nel luglio 2019 la società finanziaria **Capital One** è stata vittima di una fuga di informazioni che ha interessato 100 milioni di richieste di carte di credito, 140 000 numeri di previdenza sociale e 80 000 numeri di conti correnti bancari. Capital One ha riferito che non sono stati rivelati i numeri di carta di credito né le credenziali di accesso. La violazione ha tuttavia divulgato nomi, indirizzi, codici postali, numeri di telefono, indirizzi e-mail e date di nascita.[18]
- Nell'agosto 2019, 160 milioni di record di **MoviePass** sono stati lasciati non crittografati. Poiché il database della società non era protetto da password, sono stati rivelati i numeri di carta di credito e altri dettagli dei clienti. Il database è rimasto online per diversi giorni.[19] Nel frattempo, una massiccia fuga di dati ha rivelato 27,8 milioni di informazioni biometriche del personale detenute **dalla British Metropolitan Police, da banche e dall'industria della difesa**. Il database era amministrato da Suprema, una società che collabora con la polizia britannica.[20,21]
- Nel settembre 2019 sono stati violati più di 218 milioni di account di giocatori di **«Words with Friends»**. Il database degli utenti comprendeva dati di giocatori con sistemi Android e iOS che avevano installato il gioco prima del 2 settembre. Il team di hacker «Gnostic players» ha avuto accesso a informazioni quali nome dei giocatori, indirizzi e-mail, identità di login, ecc.[23]
- Nell'ottobre 2019 Adobe ha lasciato 7,5 milioni di record di clienti di Creative Cloud in un database non protetto. La fuga di informazioni ha riguardato gli indirizzi e-mail e lo stato dei pagamenti degli utenti.[24]
- Nel novembre 2019 Facebook ha concesso accesso improprio ai dati del profilo dei suoi 70 000 clienti a circa 100 sviluppatori di applicazioni. Uno di questi ha rubato i dati personali e li ha poi utilizzati a scopo di truffa.[25]

- Nel dicembre 2019 un **politico olandese** ha rischiato una pena a 3 anni di carcere per la violazione di 100 account iCloud di donne e la divulgazione di foto di nudo. Si è scoperto che il politico si era introdotto negli account iCloud personali delle donne con le credenziali trovate in precedenti violazioni di database pubblici.[26] Nel corso dello stesso mese i dati di oltre 10,7 milioni di ospiti del resort **Metro-Goldwyn-Mayer (MGM)** sono stati divulgati su un forum di hacking. Le informazioni trapelate comprendevano nome e cognome, indirizzi di casa, numeri di telefono, indirizzi e-mail e date di nascita dei clienti.[27]

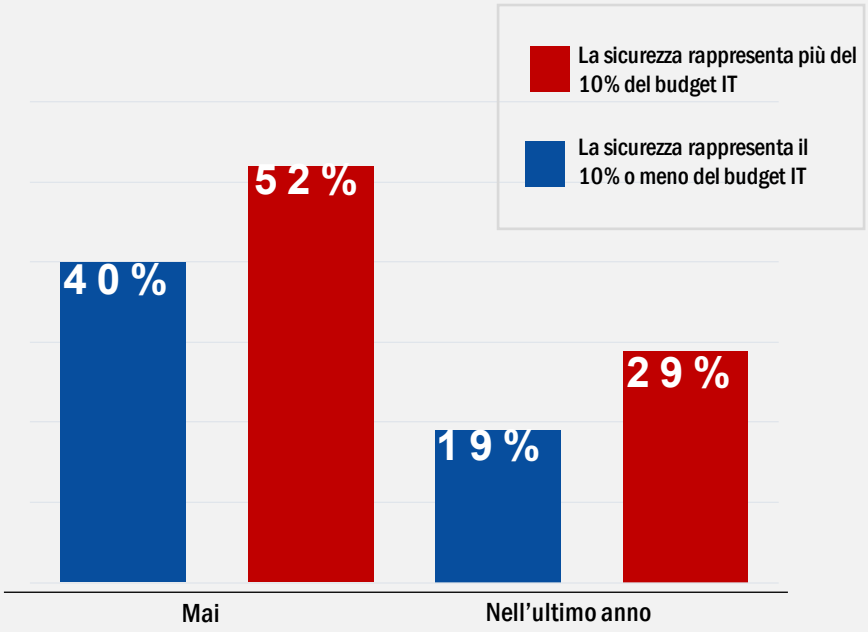


Figura 1. Tassi di incidenti di violazione per livello di spesa nella sicurezza. Fonte: CNET[14]

Vettori di attacco

_ Come

Il principale vettore di attacco nella fuga di informazioni è costituito dagli insider. Con questo termine si definisce un soggetto interessato a «esfiltrare» importanti informazioni privilegiate per conto di terzi. Altri vettori di attacco comuni utilizzati da questa minaccia sono errori di configurazione, vulnerabilità ed errori umani.

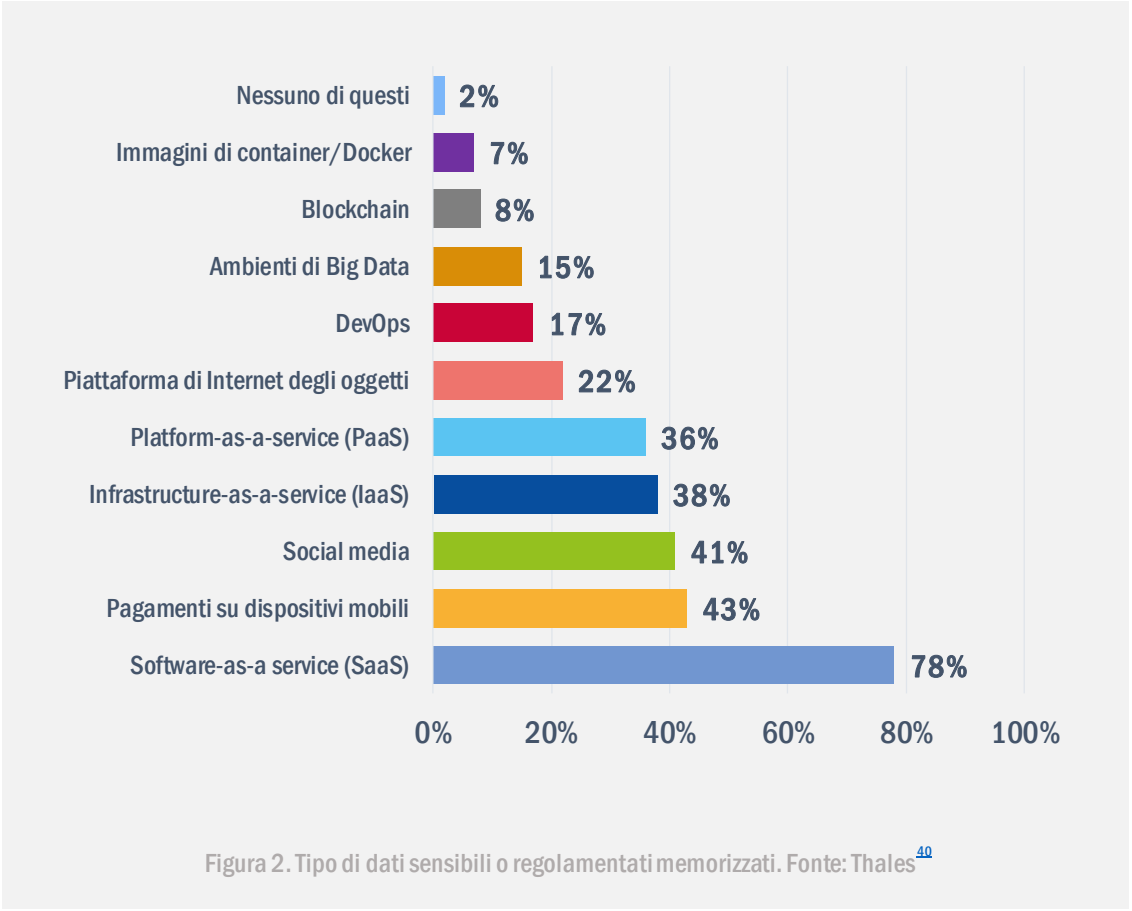


Figura 2. Tipo di dati sensibili o regolamentati memorizzati. Fonte: Thales[40]

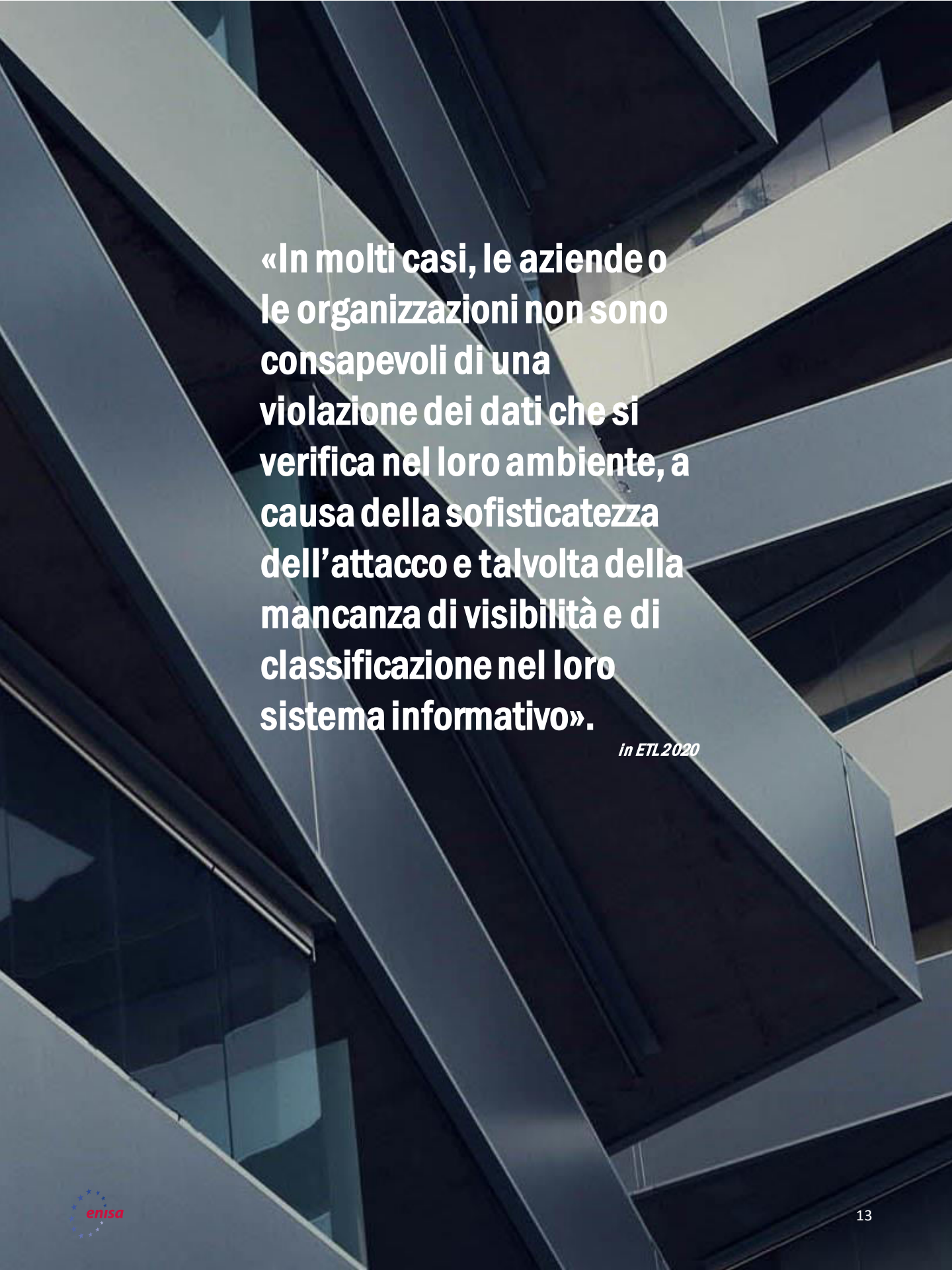
«Una violazione dei dati causa spesso una fuga di informazioni, che rappresenta una delle principali minacce informatiche, con impatto su un'ampia varietà di informazioni compromesse»

in ETL 2020

Mitigazione

Azioni proposte

- Anonimizzare, pseudonimizzare, minimizzare e cifrare i dati in conformità con le disposizioni del GDPR dell'UE, della legge californiana sulla privacy dei consumatori (California Consumer Privacy Act, CCPA) e del piano cinese di protezione multi-livello per la sicurezza delle informazioni (MLPS 2.0).[28,29,30,31] Verificare sempre gli impegni normativi per le controparti che non rientrano in iniziative bilaterali o multilaterali.[32,33,34]
- Memorizzare i dati esclusivamente su asset IT sicuri.[35]
- Limitare i privilegi di accesso degli utenti in base al principio della necessità di sapere (need-to-know).[35,36] Revocare i privilegi di accesso a chiunque non sia un dipendente.[35]
- Prevedere la formazione periodica del personale della propria organizzazione.[35,37]
- Avvalersi di strumenti tecnologici per evitare possibili fughe di dati, come ad esempio scansione delle vulnerabilità, scansione anti-malware e strumenti di prevenzione della perdita di dati (Data Loss Prevention, DLP). Implementare la crittografia dei dati e dei sistemi e dispositivi portatili e installare gateway sicuri.[36,38]
- Un piano di continuità operativa (BCP) è essenziale per gestire una violazione dei dati. Esso delinea il tipo di dati che vengono memorizzati e la loro ubicazione, e le potenziali responsabilità che potrebbero sorgere quando si attuano interventi di sicurezza e recupero dei dati. Un BCP implica una risposta efficace agli incidenti, volta ad affrontare, gestire e correggere i danni causati.[39]



«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

Riferimenti bibliografici

1. «Che cos'è una violazione dei dati e che cosa bisogna fare in caso di violazione» Commissione europea. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_it

2. «The human factor of cyber security.» CSO. https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html

3. Howard Poston. «Common causes of large breaches (Q1 2019).» 1° maggio 2019. INFOSEC Institute. https://resources.infosecinstitute.com/common-causes-of-large-breaches/#gref

4. J. Clement. «Average cost of data breaches worldwide from 2014 to 2019.» 13 agosto 2019. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/

5. «2019 Data Breach Investigations Report.» 2019. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

6. «Cyber Threatscape Report.» 2019. iDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

7. «Cybercrime will cost businesses over $2 trillion by 2019.» 12 maggio 2015. Juniper Research https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

8. «How much would a data breach cost your business?» 2019. IBM. https://www.ibm.com/security/data-breach

9. G. Dautovic. «Top 25 Financial Data Breach Statistics for 2020.» 11 marzo 2020. Fortunly. https://fortunly.com/statistics/data-breach-statistics#gref

10. Davey Winder.«Data Breaches Expose 4.1 BIllion Records In First Six Months of 2019.» 20 agosto 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#40479be4bd54

11. «Cost of a Data Breach Report.» 2019. Ponemon Institute – IBM. https://databreachcalculator.mybluemix.net/executive-summary/

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

13. Lewis Morgan. «List of data breaches and cyber attacks in February 2019 – 873,919,635 records leaked.» 26 febbraio 2019. IT Governance. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2019-692853046-records-leaked

14. Rae Hodge. «2019 Data Breach Hall of Shame: These were the biggest data breaches of the year.» 27 dicembre 2019. CNET. https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

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

16. Shelby Brown. «DoorDash data breach affected 4.9M customers, drivers, merchants.» 26 settembre 2019. CNET. https://www.cnet.com/news/doordash-data-breach-affected-4-9-million-customers-workers-and-merchants/

17. Jessica Davis. «1.9M Quest Diagnostics Patients Impacted by AMCA Data Breach.» 3 giugno 2019. HealthITSecurity https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach

18. Alfred Ng, Mark Serrels. «Capital One data breach involves 100 million credit card applications.» 30 luglio 2019. CNET. https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/

19. Shelby Brown. «Data breaches timeline: EasyJet cyberattack exposes over 9M people, and more.» 19 maggio 2020. CNET. https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/

20. 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

21. Guy Fawkes. «Report: Data Breach in Biometric Security Platform Affecting Millions of Users.» 16 giugno 2020. vpnMentor. ttps://www.vpnmentor.com/blog/report-biostar2-leak/

22. «Cost of a Data Breach Report.» 2019. Ponemon - IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

23. Oscar Gonzalez. «Zynga data breach exposed 200 million Words with Friends players.» 1 ° ottobre 2019. CNET. https://www.cnet.com/news/people-rarely-change-their-passwords-after-a-data-breach-study-says/

24. John E Dunn. «Adobe database exposes 7.5 million Creative Cloud users.» 28 ottobre 2019. Naked Security. https://nakedsecurity.sophos.com/2019/10/28/adobe-database-exposes-7-5-million-creative-cloud-users/

25. «Insider Sold 68K Customer Records to Scammers: Trend Micro.» 8 novembre 2019. CISOMAG. https://www.cisomag.com/insider-sold-68k-customer-records-to-scammers-trend-micro/

26. Catalin Cimpanu. «Dutch politician faces three years in prison for hacking iCloud accounts and leaking nudes.» 3 dicembre 2019. ZDNet. https://www.zdnet.com/article/dutch-politician-faces-three-years-in-prison-for-hacking-icloud-accounts-and-leaking-nudes/

27. Corinne Reichert. «MGM Resorts confirms data breach of 10.7 million guests.» 19 febbraio 2020 https://www.cnet.com/news/mgm-resorts-confirms-data-breach-of-10-million-guest-accounts/

28. «Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)». 27 aprile 2016. Parlamento europeo, Consiglio dell'Unione europea. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

29. «AB-375 Privacy: personal information: businesses, Assembly Bill No. 375, Chapter 55.» 29 giugno 2018. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

30. Shrub Chandrasekaran, Justin Fishman. «China's Cybersecurity Future and its Impact on U.S. Business.» 31 ottobre 2019. Jolt Digest. https://jolt.law.harvard.edu/digest/chinas-cybersecurity-future-and-its-impact-on-u-s-business

31. Reed Smith LLP. «MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates.» 9 ottobre 2019. Lexology. https://www.lexology.com/library/detail.aspx?g=36c6932b-bf41-4e08-b430-e3bc839a2328

32. «Data protection if there's no Brexit deal.» 13 settembre 2018. GOV. UK, Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

33. Eduardo Ustaran, «Brexit and data protection: Laying the odds.» 21 settembre 2018. Privacy Perspectives, iapp. https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/

34. Ibrahim Hasan. «Data protection and Brexit.» 5 settembre 2016. Gazette. https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

35. Eric Dosal. «5 Tips to Prevent Data Leakage at Your Company.» 15 marzo 2018. Compuquip Cybersecurity.https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company

36. «10 ways to protect sensitive business data.» 28 ottobre 2019. QuoStar. https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/

37. «Annual Cybersecurity Report.» 2018. Cisco https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

38. «Cybercrime tactics and techniques: Q2 2018.» 2018. Malwarebytes Labs

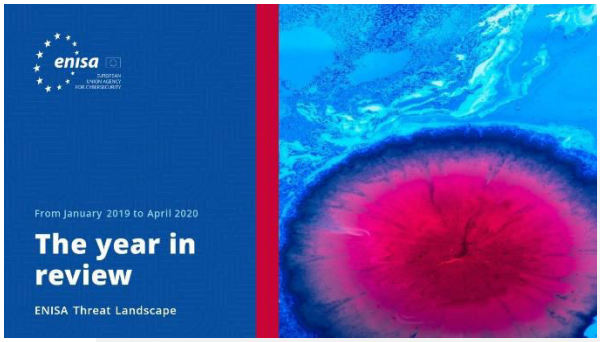
https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

39. Mona Mangat. «81 Eye-Opening Data Breach Statistics for 2020.» 27 gennaio 2020. phoenixNAP. https://phoenixnap.com/blog/data-breach-statistics

40. «2020 Data Threat Report – Global Edition.» 2020. Thales Group. https://www.thalesesecurity.com/2020/data-threat-report

41. Oscar Gonzalez. «Zynga data breach exposed 200 million Words with Friends players.» 1 ° ottobre 2019. C | net. https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

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

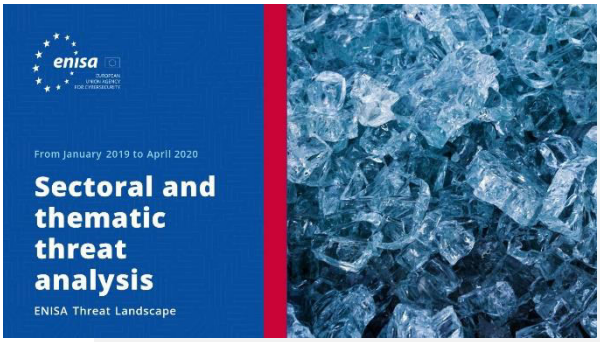
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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