Come difendersi dai rischi – La Cybersecurity

26/03/2025

Giuseppe Vacca - Rodolfo La Via
Smart-IT® - Techsystem srl

Introduzione alla Cybersecurity

Cos’è e perché e importante
Come funziona un attacco
Esempi di phishing, malware, botnet
L’evoluzione degli attacchi con l’IA

Perché investire in Sicurezza

Cosa fare in pratica

I 6 pilastri

- Formazione
- Antivirus EDR
- Backup
- Firewall
- Gestione delle vulnerabilità
- …Formazione

E altro ancora.

Cybersecurity: Cos'è è perché è importante

Cos'è la Cybersecurity? o anche … Sicurezza informatica!

E' l'insieme delle pratiche, delle tecnologie e delle strategie usate per proteggere i sistemi informatici, i dati e le reti da attacchi e accessi non autorizzati.

Proteggiamo fisicamente la nostra casa con strumenti via via crescenti:

- Fondamenta solide, Mattoni e cemento e almeno porte blindate
- Vetri antisfondamento, persiane blindate con ganci
- Antifurto interno, antifurto esterno
- Sistema di videosorveglianza
- Collegamento a centrali di monitoraggio o Carabinieri

Allo stesso modo dobbiamo proteggere il nostro Studio che contiene la nostra vita professionale e quella dei nostri collaboratori. Iniziamo dalle fondamenta che devono essere solide e aggiungiamo strumenti per aumentarne la solidità.

«Ma perché i criminali dovrebbero essere interessati proprio a me?»

Molti cyber criminali vanno a «pesca a strascico». Buttano le reti e chiunque ci finisca dentro può essere profittevole.
-> Perché quindi?
Soldi Soldi Soldi – Truffe - Terrorismo – «Baby» cyber criminali – Ritorsioni – Guerra -….

METODI PER COLPIRCI e da cosa proteggerci?

- **Phishing**
- **Furto di identità**
- **Malware**
- **Sistemi operativi vulnerabili**
- **Applicazioni vulnerabili (tra cui software «usato» a basso costo)**
- **Botnet (affaroni fatti su siti di Ecommerce, computer, tv, iot, telecamere, device in genere a prezzi pazzeschi)**
- **Applicazioni affidabili (??)**
- **Ci sono Aziende che per pochi euro vendono sul darkweb portali pronti all'uso per scatenare attacchi di ogni genere.**

SLIDE 5

Come difendersi dai rischi – La Cybersecurity

https://ransomfeed.it/?limit=ALL
https://ransomfeed.it/?page=dash-table&country=ITA

Cybersecurity: Come funziona un attacco

Internet e la posta elettronica non sono ambienti privati e sicuri; **è come camminare in una grande città; possiamo incontrare molti pericoli:**

Phishing: messaggi mail fraudolenti che ci inducono a fornire dati personali

- credenziali di accesso
- Password posta elettronica
- Documenti o informazioni aziendali
- Informazioni bancarie

il 90% delle violazioni di dati inizia con e-mail di phishing.

Spesso basta un solo click per essere compromessi o per esporre dati sensibili.

Nell’86% delle Aziende almeno un utente *abbocca*.

SLIDE **8**

Qualche esempio, furto di credenziali o dati bancari

Da: Noreply Service <cs@solcellskompaniet.se>
Inviato: venerdì 12 gennaio 2024 22:26
A: nome.cognome@azienda.it
Oggetto: Friday, January 12, 2024

Support-Desk

Hi Nome Cognome,
The Password; for nome.cognome@azienda.it needs to be revalidiated today
Time: (Friday, January 12, 2024 1:26 PM!)
Tick the box below, to continue with the same password,
KEEP MY CREDIENTIALS

Da: Service.Desk- <luismontes@latiendacom.com>
Inviato: lunedì 15 gennaio 2024 16:44
A:
Oggetto: Notification Storage LImit

Microsoft

Storage Is Almost Full.

96GB 99GB

Email Storage Quota Exceeded.
You must immediately clear your cache in order to send and receive new mails.

Clear Cache Now

NOTICE: If the cache is not cleared, incoming messages will be rejected.

Microsoft Postmaster Delivery System

MS Corporation, One MS Way, Redmond, WA 98052

Da: Area Clienti e Rinnovi <support@celtempimoderni.it>
Inviato: martedì 28 maggio 2024 06:08
A: - Info <info@
Oggetto: comunicazioni@staff.aruba.it

aruba.it

Gentile Cliente

Ciao,
ti informiamo che il dominio a cui risulta collegato questo account di posta, scadrà il giorno ***28/05/2024.***

Desideriamo ricordare che, qualora il dominio non venga rinnovato entro tale data, questi e tutti i servizi associati, comprese le caselle di posta verranno disattivate e no npotranno più essere utilizzate per l'invio e la ricezione.

Fattura N : 123653914
Importo dovuto: 4,37€
Data di scadenza:28/05/2024

Puoi accedere alla tua area clienti per visualizzare e pagare la fattura su

RINNOVA IL DOMINIO

Altre considerazioni:

- Se ricevete mail da fantomatici professionisti verificate i dati (indirizzo mail, indirizzi fisici, nomi) perché, se phishing, sono sempre falsi!
- Mail contenenti scansioni che arrivano dal nostro scanner/stampante

Malware

Tramite mail fraudolente, i cybercriminali possono indurci ad aprire un allegato o cliccare su un link.
In pochi secondi il nostro PC sarà sotto il controllo dell'attaccante il quale potrà:

- Ricercare le vulnerabilità di tutti i dispostivi della rete e attaccare altri dispositivi interni
- Rubare i dati
- Registrare tutto quello che viene digitato sulla tastiera
- Accesso alla webcam e al microfono
- Recupero delle credenziali salvate sul browser
- Installazione di ulteriori software «spia» che analizzano la rete interna

Spesso l'attaccante rimane nascosto per lungo tempo prima di passare alle fasi finali dell'attacco:

- Eliminare i backup individuati
- Criptare tutti i dati per chiedere un riscatto

SLIDE 11

Qualche esempio, malware

Da: parte <aksilxinicn@outlook.com>
Inviato: 6 ottobre 2023 10:09
A: nome.cognome@azienda.it
Oggetto: Commissione di vigilanza sul registro tributario

Gentile Nome Cognome,

dall'esame dei dati e dei saldi relativi alla Divulgazione delle liquidazioni periodiche Iva, da lei mostrate per Il trimestre 2023, risultano emerse alcune incoerenze.
Le notificazioni relative alle sconvenienze riscontrate sono disponibili nel "Cassetto fiscale" (sezione l'Agenzia)
disponibile dal sito internet dell'Agenzia delle Entrate (www.agenziaentrate.gov.it) e in versione intera nell'archivio incluso alla attuale e-mail.

http://clinicamomentum.com.br/documenti/TFLxilzhXPpufRHZ

La presente e-mail è stata riprodotta automaticamente , pertanto la preghiamo di non dare risposta a tale indirizzo di posta elletronica.

Ufficio accertamenti,
Direzione nazionale Agenzia delle Entrate

Da: noreply©inbank.it <hw4fun@higiworks.pt>
Inviato: venerdì 27 agosto 2021 13:21
Oggetto: Inbank - Alert bonifico
Priorità: Alta

INBANK
VIA JACOPO ACONCIO,
9 - 38122 TRENTO,
ITALIA | P. IVA 02529020220|
C.F. 01761610227

INBANK

Ti abbiamo notificato questo pagamento secondo le istruzioni dei nostri clienti e ti abbiamo inviato una copia del pagamento. L'importo totale pagato è di 7.640,00 euro
Riferimento transazione: 3904878395093859
ti confermiamo che il giorno 27/08/2021 alle ore 09:06 dal conto IT69F0878476440010003517711 è stato inviato un bonifico con importo 7.640,00 euro
Vedere la copia allegata per maggiori dettagli

facebook FOLLOW US

Nota: INBank non richiede mai la password del conto bancario o informazioni riservate sulla carta di credito.

Se sei nostro cliente, scarica l'ultima app mobile con i pulsanti sottostanti.

App Store Google Play

Come faccio a sapere che questa email non è contraffatta?
Si ricorda che al fine di tutelare maggiormente i propri clienti, Inbank non chiederà mai le credenziali di accesso all'area riservata tramite posta elettronica. Fai attenzione alle email che chiedono di fornire dati personali sensibili con urgenza: solitamente rappresentano un tentativo di frode. Inoltre, le email fraudolente spesso contengono errori di ortografia e grammaticali. Ricorda di non cliccare mai link che sembrano sospetti.

Comunicazione riservata
Ai sensi del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("GPDR"), le informazioni contenute nella presente email ed ogni relativo allegato devono intendersi indirizzate unicamente al destinatario indicato in quanto potrebbero contenere dati riservati, confidenziali e non divulgabili a terzi. Qualora il lettore del presente messaggio non sia il destinatario previsto o un dipendente o altro personale addetto al recapito del presente messaggio al suo destinatario, si informa che è vietato e costituisce illecito perseguibile ai sensi di legge (art. 616 c.p.) qualsiasi utilizzo, divulgazione, distribuzione o riproduzione della presente comunicazione. Qualora abbiate ricevuto per errore il presente messaggio, siete invitati a comunicarlo immediatamente dandone avviso via email (info @ allitude. it) ed a cancellare il documento originale da ogni computer astenendovi dal trattenerne copia.

Important information on security
You are hereby reminded that, in order to offer better protection to clients, Inbank never asks for your access code to the reserved area via email. Furthermore, the Bank never sends messages that explicitly require connection to internet sites.

Email disclaimer
Pursuant to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GPDR"), this email (including any attached documents) is proprietary, confidential and intended only for the named recipient(s). This email may contain confidential or privileged information. If you are not the intended recipient, you may not review, retain, copy, disclose or distribute this message, and the sender kindly asks you to notify the sender by replying to info @ allitude. it immediately and delete this message from any computer.

SLIDE **12**

Qualche esempio, malware

Rispondi Rispondi a tutti Inoltra

mercoledì 02/02/2022 10:18

IM

Il Ministro degli Interni <IlMinistrodeglilr

Restrizioni anti-Covid19

A nome.cognome@azienda.it

I collegamenti e altre funzionalità all'interno del messaggio sono stati disabilitati. Per riattivare le funzionalità, spostare il messaggio nella cartella Posta in arrivo.
Outlook ha bloccato l'accesso ai seguenti allegati potenzialmente pericolosi: documento_26.zip.

Gentile Nome Cognome,

Il Ministro degli Interni;
mette a disposizione per le attività presenti sul territorio italiano un file di testo contenente le linee guida per le restrizioni anti-Covid19 in vigore dal 01/02/2022, scaricabile in allegato.
Si ricorda ai gentili cittadini che il mancato rispetto delle nuove restrizioni comporterà delle sanzioni penali , anch'esse elencate in allegato.

password: Covid#19

La presente e-mail è stata generata automaticamente, quindi la preghiamo di non rispondere a questo indirizzo di posta elettronica .

Polizia di Stato — POLIZIA — MINISTERO DELLA DIFESA REPVBBLICA ITALIANA — EUROPOL — INTERPOL

DIREZIONE CENTRALE DELLA POLIZIABRIGATA DI PROTEZIONE MINORI

GARANZIA DI PROCEDURA LEGALE

Alla tua attenzione:

Io sottoscritto Sig. **Lamberto Giannini**, Capo della Polizia e direttore generale della Pubblica Security in collaborazionecon la Sig.ra Catherine De Bolle, Direttore di Europol e Capo della Brigata Protezione Minori (BPM) visti **gli articoli 20 21-1 e da 75 a 78 del Codice di Procedura Penale**.

Ti inviamo questo mandato poco dopo un sequestro informatico dell'infiltrazione informatica per informarti che seioggetto di diversi procedimenti legali in vigore.

Intraprendiamo azioni legali contro di te per:

- Pornografia Infantile
- Pedofilia
- Esibizionismo
- Cyberpornografia
- Offesa Alla Decenza

Per vostra informazione, **la legge 3901 del codice di procedura penale del marzo 2007** aumenta le pene quandosiano state commesse proposte, aggressioni sessuali o stupri.

Hai commesso il reato dopo essere stato preso di mira su Internet (sito pubblicitario), aver visualizzato un sito di pornografia infantile, foto/video di nudo e i tuoi scambi sono stati registrati dal nostro cyber-gendarme e costituiscono laprova dei tuoi reati.
La corte di giustizia che condanna tutti i tentativi relativi al traffico sessuale non ha potuto trascurare alcuno sforzo sutale vandalismo.

In virtù degli **articoli n. 98-468 del 17 giugno 2007, art. 809 comma 15 cp - Gazzetta Ufficiale 11 giugno 2009**

Chiunque compia tali atti è passibile di procedimenti giudiziari e di una pena da **5 a 10 anni** di reclusione e **di una multada 5.000 a 76.000 euro.**

Per motivi di riservatezza ti inviamo questa e-mail, sei pregato di farti sentire via e-mail scrivendo le tue giustificazioniaffinché siano esaminate e verificate al fine di valutare le sanzioni; questo entro un termine rigoroso di 72 ore.

Siete pregati di risponderci via e-mail scrivendo le vostre giustificazioni affinché vengano messe all'esame e verificate alfine di valutare le sanzioni che entro un termine rigoroso di 72 ore.

Trascorso questo tempo, saremo obbligati a inviare la nostra denuncia al Pubblico Ministero per stabilire un mandatod'arresto nei vostri confronti e procederemo al vostro immediato arresto.

In questo caso, la tua pratica sarà trasmessa anche alle associazioni per la lotta alla pedofilia e ai media per la pubblicazione in modo che la tua famiglia e i tuoi cari sappiano cosa stai facendo, sarai registrato come molestatoresessuale in tutte le amministrazioni in tutta Europa e nel **Registro Nazionale dei Reati Sessuali (RNDS).**

Stiamo ancora aspettando la tua email di ritorno per dirti come procedere.

Cordiali saluti,
Sig. Lamberto Giannini
Capo della Polizia e direttore generale della Pubblica Security

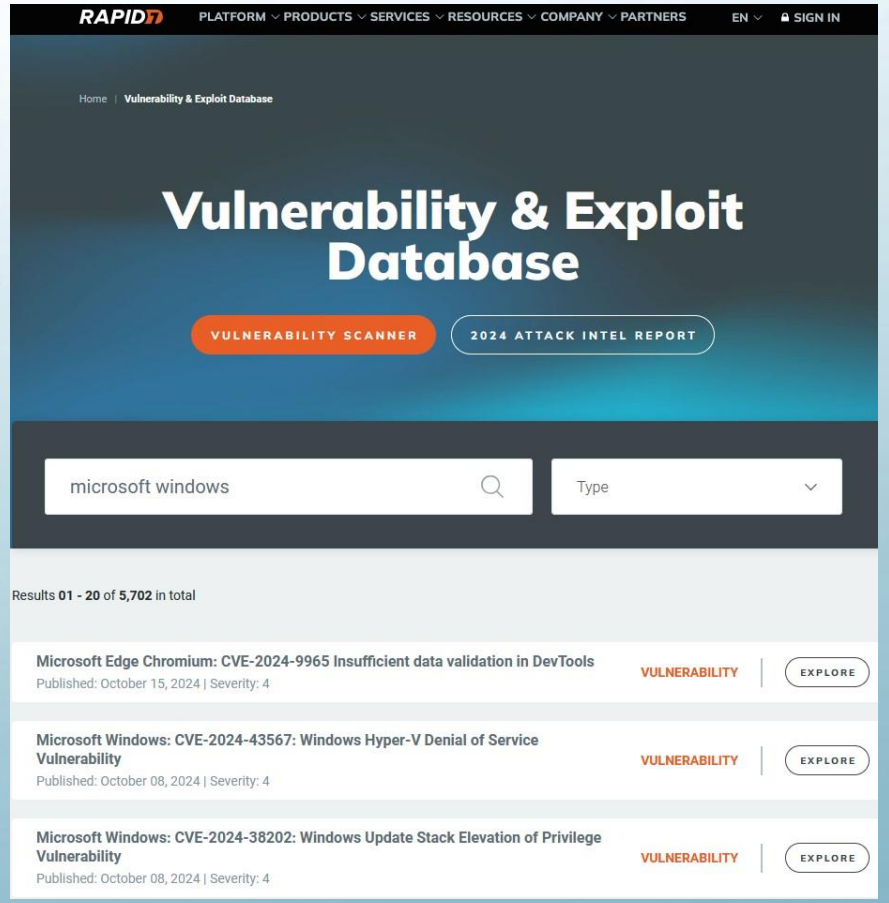
DIREZIONE CENTRALE DELLA POLIZIABRIGATA DI PROTEZIONE MINORI
Via Portuense, 1680, 00148 Roma RM, Italie

Vulnerabilità - cosa sono e come vengono sfruttate dai cybercriminali

Ogni software può contenere errori di programmazione, punti deboli o falle che i cybercriminali possono sfruttare per prendere il controllo di un computer.

Su internet esistono librerie pubbliche che contengono programmi già pronti, chiamati **exploit**, progettati appositamente per sfruttare queste vulnerabilità. Quando un exploit viene eseguito sul computer della vittima, permette spesso al malintenzionato di ottenere il controllo completo del sistema.

Ogni giorno sono individuati centinaia di nuovi exploit su ogni tipo di software, per questo è fondamentale programmare sistematicamente le attività di Vulnerability Assessment.



Botnet

Sono reti di milioni di device compromessi che vengono pilotati all'occorrenza per effettuare attacchi mirati spesso senza che i possessori si accorgano di nulla!

Ad esempio, in occasione di un evento particolare in cui la visibilità su internet è fondamentale, potreste voler bloccare i siti dei vostri concorrenti. Noleggiate una botnet che li colpisca in un dato giorno e per un certo periodo.

Applicazioni affidabili ?? Un esempio TikTok…

Cioè? Perché l'America ce l'ha tanto con Tiktok?

Negli Stati Uniti TikTok ha circa 170 milioni di utenti (su 350Mil di abitanti). In Italia sono circa 21 milioni. In Europa circa 230 milioni (su 750 Mil di abitanti).

Secondo Voi, cosa succederebbe se ci fosse una guerra tra Cina e Occidente?

Un minuto dopo la Cina potrebbe spegnere tutti i nostri cellulari (e stiamo parlando solo di tiktok, vedi altri device). Oppure utilizzarli per effettuare attacchi coordinati a tutte le infrastrutture critiche…

Cybersecurity: Evoluzione degli attacchi con l'IA e nuove tecniche di Phishing

Cybercriminali nell'era dell'IA e nuove tecniche di Phishing

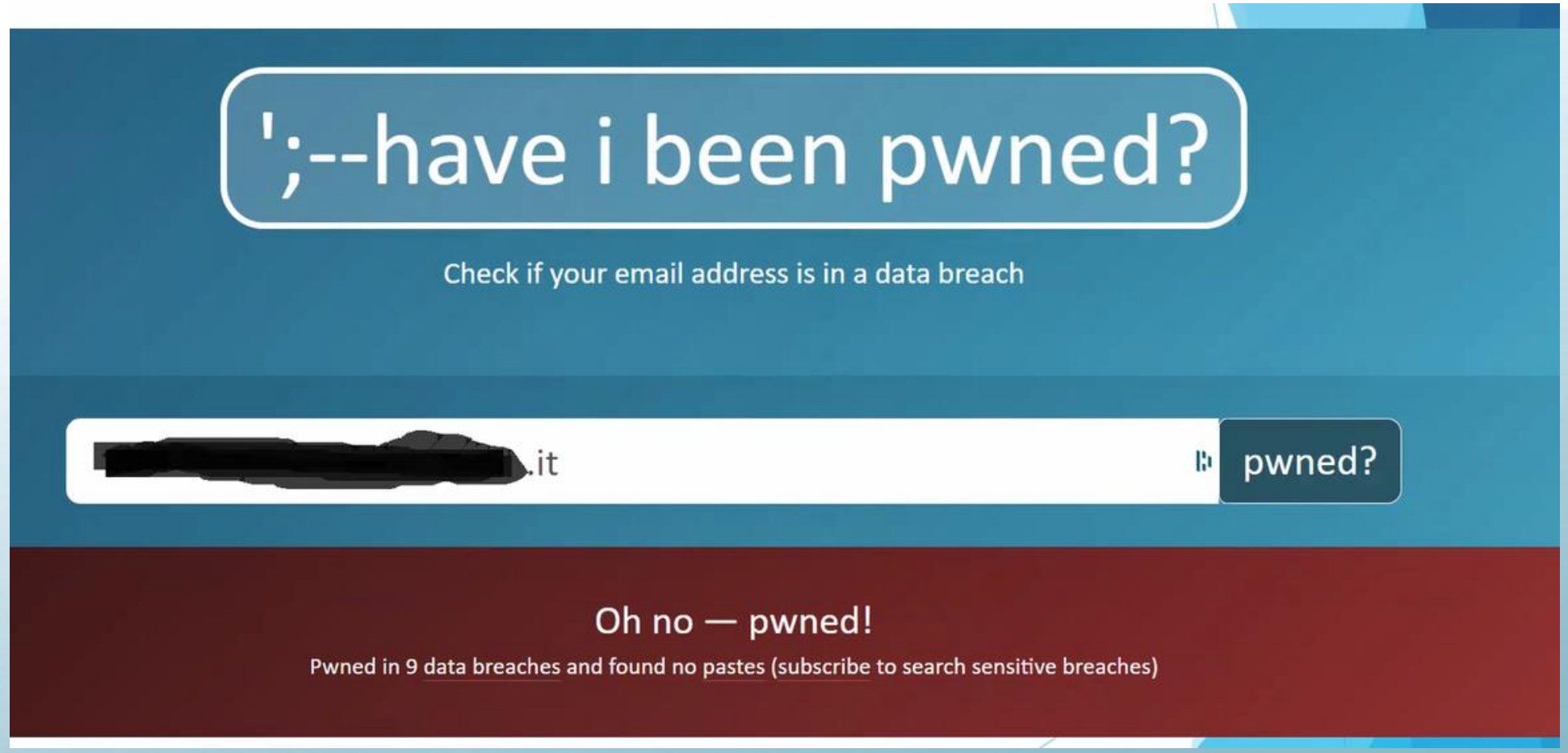
l'Intelligenza Artificiale (IA) ha modificato profondamente il mondo della sicurezza informatica. I cybercriminali hanno accesso a strumenti sempre più potenti, che rendono le loro attività più rapide ed efficaci.

Se l'IA offre nuove opportunità alle aziende, ne crea altrettante per i criminali informatici. Ad esempio:

Creazione di malware – Con l'IA, è possibile creare programmi dannosi (malware) in modo più veloce e sofisticato.

Phishing più realistico – L'IA permette di automatizzare campagne di phishing, con testi scritti in un linguaggio sempre più naturale e credibile.

Come difendersi dai rischi – La Cybersecurity



Negli ultimi mesi hanno preso piede nuove tecniche di phishing

(fonte: Alessandro Vannini – The Phoenix -Admin Ethical Hacker)

Una delle nuove tecniche è il QRCODE Phishing.

E’ impossibile intrepretare cosa c’è scritto dietro un QR code. Questo facilita il camuffamento e li fa diventare degli ottimi vettori di phishing

Pensate solamente ad un QR code di un ristorante oppure in un luogo con alto afflusso di persone. Se lo sostituisco posso fare quello che voglio, magari chiedere delle credenziali, scaricare un pdf o un link con un malware, chiedere il pagamento su conti falsi.

Cosa c’è dietro il QR qui a fianco?
Potete provare ad inquadrare questo se volete ;-)

Quindi come mi comporto?

- **Controllare link senza aprirlo**
  - Alcune app mostrano l'URL prima di aprirlo. Se sembra sospetto (domini strani, caratteri anomali, URL accorciati), evita di aprirlo.
- **Evitare QR Code su adesivi**
  - Magari è stato incollato sopra un nuovo codice malevolo (anche in luoghi apparentemente innocui)
- **Non inserire mai dati sensibili**
  - … o informazioni di credenziali varie e comunque verificare che l'URL sia legittimo
- **App di scansione con funzioni di sicurezza**
  - Alcune app includono controlli di sicurezza per cercare di rilevare link dannosi (es. malwarebyte)

Malwarebytes ed il QR scanner

https://www.malwarebytes.com/blog/news/2019/07/qr-code-scam-can-clean-out-your-bank-account

Malwarebytes ha un QR code scanner per mobile in grado di riconoscere i link nocivi.

Gli URL abbreviati

Vi sarà capitato di vedere in alcuni post dei link che non sono propriamente lunghi.

Gli URL abbreviati sono fatti per risparmiare spazio negli annunci pubblicitari.
La loro utilità, cela una potenziale minaccia in quanto non si riesce a risalire direttamente all'indirizzo principale.
https://bit.ly/3WQKI3P
Per capirci, questo link **https://bit.ly/3WQKI3P** porta al sito Microsoft.
Ci sono molti altri tipi di link «corti»

- **goo.gl** di Google
- **tinyurl.com**

- Proviamo a mettere il link su https://www.virustotal.com/gui/
  - Usiamolo sempre, c'è anche APP per il mobile

IA nel phishing audio

In ambito Audio l'IA ha raggiunto quasi un livello di perfezione. Posso cambiare la mia voce anche in tempo reale (per ora non sul VOIP).

Inoltre siamo ormai abituati ad una scarsa qualità della voce (da quando abbiamo pensionato il telefono su rete dedicata).

Ci sono servizi che clonano e cambiano la voce in tempo reale. Campiono 2 minuti di voce e mando il testo! E sarà sempre peggio.

Esempi:
Evenlabs - https://elevenlabs.io/?ref=Welcome.AI
SUNO - https://suno.com/create?wid=default

Perché investire in Sicurezza?

Perché investire in Cybersecurity?

- **Protezione dei Dati Sensibili dei Clienti**
  - I Professionisti gestiscono dati altamente sensibili. Un attacco potrebbe esporli con conseguenti danni economici e legali

- **Reputazione e Fiducia**
  - Un incidente di sicurezza può danneggiare gravemente la reputazione dello studio e far perdere fiducia e Clienti preziosi

- **Prevenzione dei Costi di Ripristino**
  - Una compromissione può essere molto costosa da risolvere (sempre che sia possibile!): recupero dati, ripristino sistemi, danni legali e gestione del Databreach

Perché investire in Cybersecurity?

- **Obblighi Normativi e Sanzioni**
  - IL GDPR e la NIS2 impongono standard di sicurezza elevati. La mancata conformità espone a pesanti sanzioni amministrative di rilievo anche penale. Inoltre la NIS2 richiede la conformità anche alla supply chain.

- **Riduzione del Rischio di Interruzione delle Attività**
  - Un attacco informatico può bloccare l'accesso ai sistemi e ai documenti, interrompendo l'operatività dello studio per giorni, per settimane… o per sempre.

- **Cybersecurity Come Vantaggio Competitivo**
  - Essere proattivi nella protezione dei dati può diventare un vantaggio competitivo. Comunicare ai clienti che lo studio segue pratiche di sicurezza avanzate dimostra serietà e attenzione alla protezione dei loro interessi.

Perché investire in Cybersecurity?

- **Solo qualche esempio…**
  - Hacker contro studi commercialisti: danni estesi a tutta Italia
    - Link fonte
  - Milano, l'offensiva hacker contro gli studi dei commercialisti (che pagano il riscatto)
    - Link fonte (milano.corriere.it)
  - CNPR, segnalato un attacco informatico
    - Link fonte (fiscal-focus.it)

Ma perché qualcuno dovrebbe essere interessato al mio Studio?

- Gli attacchi non sono mirati solo alle grandi aziende. Anzi… le piccole spesso non investono in sicurezza e sono un bersaglio più facile. Se pesco a strascico colpisco chi è meno preparato. I cybercriminali non cercano grandi Aziende, cercano dati.
- Dati sensibili = Interesse dei criminali
- Spesso sento dire: Ma a chi vuoi che interessi il bilancio del mio Cliente? I dati personali finanziari hanno un enorme valore di mercato. Possono essere usati per truffe, furti di identità. I cybercriminali non cercano grandi Aziende, cercano dati.
- Minore protezione = Obiettivo più facile
- Costi elevati di recupero
- Per una piccola attività un attacco può essere devastante e i costi possono essere insostenibili. Spesso è più «conveniente» pagare il riscatto. Attenzione però…
- Attacchi automatizzati: la maggior parte degli attacchi sono automatizzati.

Cosa fare in pratica?

I 6 Pilastri:

1. Formazione
2. Antivirus EDR
3. Backup
4. Firewall NGFW
5. -> Aggiornamento dei sistemi e degli applicativi (Vulnerability Assessment)
6. …Formazione

E inoltre:

- Password forti (aggiornate di frequente) e autenticazione a due fattori (2FA o MFA) (attenzione: SMS sono molto deboli e anche MFA può essere superato)
- Se le mail sono vitali in ingresso e uscita: Archiviazione mail
- Policy per l'uso degli asset IT Aziendali (strumenti e altro)
- Acquisti sicuri
- Gestione dei Log
- Archiviazione vecchia posta elettronica
- Attenzione alla dismissione di pc e dispositivi vari

… i servizi devono sempre essere gestiti e monitorati da un esperto:

➔ Un backup non controllato non serve a nulla o meglio quando serve, non funziona!

➔ un Firewall non aggiornato o lasciato per suo conto è quasi come non averlo

Possibilmente, se non avete competenze interne, **sottoscrivete servizi gestiti (con un MSP)** e/o richiedeteli al vostro fornitore/consulente IT.

Antivirus EDR (EndPoint Detection and Response) … non solo Antivirus

Proprietà	Antivirus Tradizionale	EDR
Metodo di rilevamento	Basato su firme (confronta file con un database di minacce conosciute)	Analisi comportamentale e intelligenza artificiale per identificare attività sospette
Risposta alle minacce	Elimina o mette in quarantena file dannosi	Rileva, analizza, blocca e fornisce strumenti per rispondere agli attacchi
Protezione contro minacce nuove o avanzate	Limitata alle minacce già note	Più efficace contro attacchi zero-day e malware avanzato
Monitoraggio in tempo reale	Limitato	Completo, con raccolta e analisi dei dati di sicurezza
Visibilità e analisi	Nessuna o minima	Dashboard centralizzata con informazioni dettagliate sugli attacchi

📌 **Esempio pratico:**
Se un attacco ransomware tenta di crittografare file in un sistema, un antivirus tradizionale potrebbe non riconoscerlo subito se il malware è nuovo. Un **EDR, invece, rileva l'attività anomala** (modifica massiva di file) e la blocca prima che il danno sia irreparabile.

🆓 **Strumenti gratuiti:**
➔ Wazuh : EDR open-source e freeware con SIEM integrato. https://wazuh.com/
➔ OSSEC: https://www.ossec.net/

🔷 **Conclusione:** Se un antivirus è come un guardiano che controlla chi entra e chi esce da un edificio, un **EDR è un investigatore che monitora continuamente cosa succede dentro e interviene in caso di attività sospette.**

Backup

Un attacco informatico, un errore umano o un guasto hardware possono causare la perdita di dati cruciali. **Un backup regolare e sicuro è la migliore difesa!**
Passaggi chiave:

- Identificare i dati critici - documenti, DB, email, ERP, applicazioni….
- Automatizzare i backup - no soluzioni manuali
- Backup in cloud – evitare backup solo su dispositivi locali (rischio ransomware, guasti), non farli su chiavette e HD esterni (databreach)
- Regola del 3-2-1
  - 3 copie dei dati (originale + 2 backup)
  - 2 tipi di supporto diversi (NAS + Cloud)
  - 1 backup offsite (Cloud o datacenter)
- Monitorare quotidianamente esiti e simulazioni di ripristino periodiche

FREE **Strumenti gratuiti:**

➔ https://duplicati.com/
➔ Veeam Backup (Community Edition)
➔ https://www.urbackup.org/

🔷 **Conclusione:** Un backup ben fatto è la miglior difesa contro ransomware e perdite di dati!

Firewall NGFW

Un **Next-Generation Firewall** non si limita a filtrare il traffico di rete in base a porte e indirizzi IP, ma include funzionalità avanzate come:

- **Ispezione del traffico a livello applicativo** → Riconosce e filtra il traffico di applicazioni specifiche (es. bloccare WhatsApp o controllare il traffico di Office 365).
- **Intrusion Prevention System (IPS)** → Rileva e blocca attività sospette o attacchi informatici in tempo reale.
- **Analisi comportamentale e machine learning** → Riconosce minacce avanzate, anche sconosciute
- **Filtro URL e protezione Web** → Blocca siti dannosi e phishing.
- **Decryption SSL/TLS** → Analizza il traffico crittografato per individuare malware nascosti.
- **Integrazione con EDR e SIEM** → Collabora con sistemi EDR) e Security Information and Event Management (SIEM) per una protezione più completa.

📌 Esempio pratico:

Se un dipendente scarica un file da un sito web dannoso, un **firewall tradizionale** potrebbe non bloccarlo, mentre un **NGFW** lo riconosce come pericoloso e impedisce il download.

🆓 Strumenti gratuiti:

➔ PfSense: Include funzioni di **stateful firewall, VPN, IDS/IPS, filtro web, VPN**

➔ OpnSense: Include funzioni di **stateful firewall, VPN, IDS/IPS, filtro web, VPN, DPI, Netflow, reporting**

🔷 Conclusione:

Un **NGFW è essenziale per le aziende moderne**, perché offre **protezione avanzata contro attacchi sofisticati**, mantenendo le reti più sicure rispetto ai firewall tradizionali.

Aggiornamento dei sistemi e degli applicativi
Vulnerability Assessment e Remediation Plan

Non basta aggiornare «windows» ogni tanto. Tutte le applicazioni installate nel PC devono essere aggiornate. Questo perché, come già evidenziato precedentemente, ogni applicazione (anche WinZip o Acrobat PDF Reader) può essere un cavallo di troia.
Un'attività di «vulnerability assessment» deve comprendere:

- Individuazione automatica di tutti i device nella rete
- Scansione completa delle vulnerabilità
- Descrizione completa delle vulnerabilità rilevate
- Piano di Remediation (possibilmente con indicazione di priorità
- Conformità GDPR e NIS

e, per essere a norma, tutte le attività dovrebbero essere documentato e certificate.

FREE **Strumenti gratuiti:**
➔ https://www.openvas.org/
➔ Nessus Essentials https://www.tenable.com/

🔷 **Conclusione:** un'attività ricorrente di scansione delle vulnerabilità e relativa applicazione del piano di Remediation contribuisce ad elevare enormemente il grado di sicurezza della propria rete.

… e inoltre:

Password forti:

- Non usate mai la stessa password per accedere a più servizi.
  - FREE https://haveibeenpwned.com/
  - FREE https://keepass.info/

… e inoltre:

Autenticazione a due fattori (2FA o MFA):

- Ovunque possibile abilitate l'autenticazione almeno a 2 fattori. Ad esempio per l'accesso alla vostra posta elettronica. -95% di compromissioni. Es. FREE google authenticator

Archiviazione delle email:

Se le mail in ingresso e uscita sono fondamentali un sistema di backup può non bastare! E' necessario un sistema di archiviazione in tempo reale. Ad esempio FREE https://www.mailstore.com/en/products/mailstore-home/ (att. all'uso commerciale)

Gestione dei LOG:

I log di sistema sono una miniera di informazioni preziose. **Analizzarli permette di individuare attacchi informatici, errori e comportamenti sospetti prima che causino danni.**

FREE https://graylog.org/

… e inoltre:

Acquisti sicuri:
Acquistate il materiale informatico da fornitori «sicuri» e che garantiscano la provenienza ufficiale della merce da canali di distribuzione ufficiali. Si… forse li pagherete di più ma sarete sicuri di non essere «voi stessi» il prezzo da pagare!

Formazione:
Fate formazione continua ai vostri collaboratori, magari simulando anche una campagna di phishing ad hoc per poi spiegare agli utenti i comportamenti da tenere e da evitare. Ricordate loro che un attacco grave al vostro Studio può compromettere anche il loro lavoro!

Iniziative Camera di commercio:
Cybersecurity PMI 2025
www.to.camcom.it/cybersecurity-pmi

I cybercriminali hanno tutto il tempo che vogliono e molte risorse economiche.
Non possiamo competere.

La Cybersecurity non è un lusso per pochi, ma una necessità anche per i piccoli.

Basta un singolo incidente per causare danni *difficili* da gestire.

Investire in sicurezza significa proteggere non solo i dati, ma anche la propria reputazione, i collaboratori, i clienti e il futuro della propria attività.

GRAZIE

Domande e Risposte

Come difendersi dai rischi – La Cybersecurity

GRAZIE …

www.odcec.torino.it
www.linkedin.com/company/odcec-torino/
www.youtube.com/channel/UCBUHnLEOEHA6YY-MLr8vG8A/videos