DAL CUORE DELLO STATO

il Governatorato si racconta

Anno 2 Città del Vaticano Numero 2

TRIMESTRALE APRILE-GIUGNO 2025

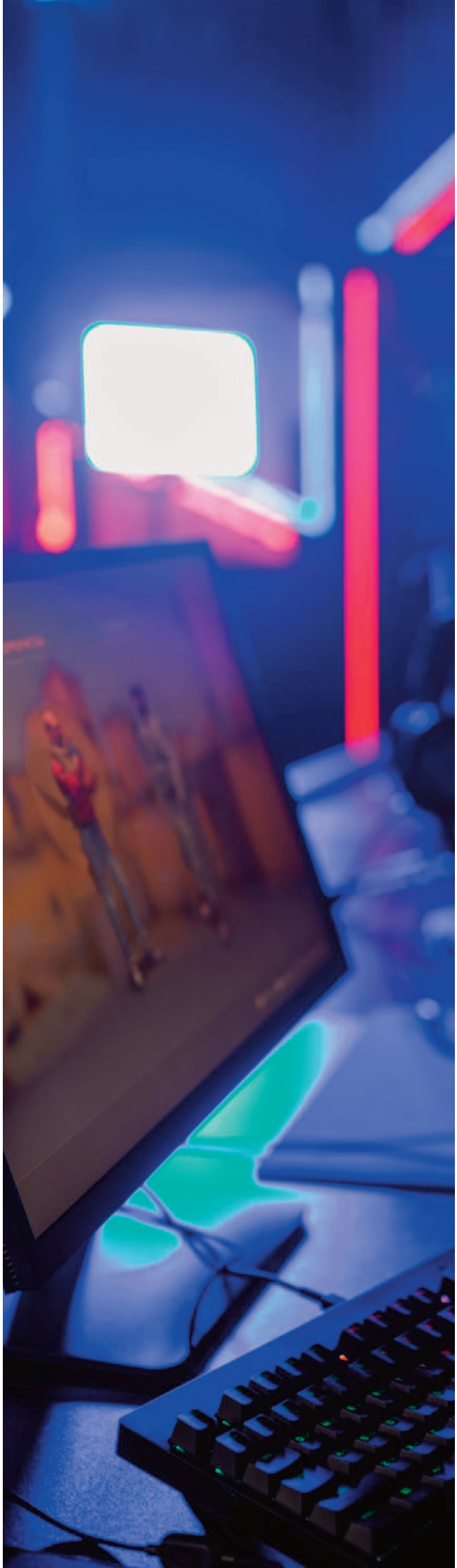
Pubblicato dal Governatorato dello Stato
della Città del Vaticano

Comunicazione Istituzionale
00120 Città del Vaticano
(Stato della Città del Vaticano)
Email: comunicazione@scv.va

Sito internet: www.vaticanstate.va

X (Twitter): Governatorato_SCV
Instagram: Governatorato_SCV

Responsabile editoriale: Nicola Gori
Editore: Governatorato dello Stato della Città del Vaticano



LA SICUREZZA INFORMATICA È RESPONSABILITÀ DI CIASCUNO

La scelta di dedicare questa newsletter alla cybersicurezza è nata dal desiderio di offrire una sorta di vademecum per orientarsi e tutelarsi in una realtà complessa e multiforme. Convinti che a livello personale, ognuno, ha una parte di responsabilità per la sicurezza informatica.
In effetti, considerate le loro implicazioni, le questioni relative alla sicurezza informatica vanno ben oltre le modalità tecniche. Interessano, tra l'altro, varie dimensioni: la gestione del rischio, il diritto, la comunicazione, la privacy, l'economia, ecc.
È evidente che la sicurezza informatica è un settore molto specifico, che coinvolge esperti in informatica, matematica o fisica. Tuttavia, essa ormai fa parte del nostro quotidiano, come ne fanno parte il mondo digitale e, ultimamente, l'Intelligenza artificiale. Si occupa della protezione di sistemi informatici, reti, dati e dispositivi da minacce cibernetiche, attacchi e violazioni della privacy. È al servizio della garanzia della confidenzialità, della disponibilità delle risorse digitali, per impedire danni e garantire protezione e sicurezza a tutte le attività nell'ambiente digitale.
In questo contesto, è indispensabile avere la consapevolezza che all'interno del Governatorato, dove si usano strumenti informatici, ognuno ha una parte di responsabilità nella protezione della struttura.
In questa newsletter si possono trovare alcuni utili accorgimenti, che un gruppo di esperti del settore suggerisce di applicare alla nostra relazione quotidiana con il mondo cibernetico. Tra le indicazioni fondamentali, la particolare attenzione da riservare alle richieste di cui non si conosce l'origine, agli allegati e ai supporti USB potenzialmente inattivi. In caso di dubbio è sempre bene chiedere consiglio e avvisare il responsabile della sicurezza.

In effetti, gli attacchi informatici possono avere effetti molto negativi sull'integrità della struttura digitale. I cyberpirati mirano a procurarsi vantaggi di natura finanziaria, come nel caso di attacchi ransomware. Ma, tendono anche a ottenere informazioni riservate che producono effetti sulle persone. È il caso di dati personali sottratti (ad esempio: furto d'identità) e ceduti a organizzazioni criminali per i loro scopi.

Inoltre, l'attacco subìto da una realtà istituzionale può anche danneggiare la fiducia nei suoi confronti e, quindi, quando un sito internet viene colpito, vi è sempre una ricaduta a livello di immagine.
Se si arriva poi alla compromissione dell'integrità dei sistemi informatici, a volte, è il funzionamento stesso dell'organizzazione a risentirne. Gli attacchi possono anche avere effetti devastanti, quando l'obiettivo è il sistema di un ospedale o di un servizio di trasporto.
Per tutte queste ragioni, è opportuno essere informati e consapevoli della responsabilità personale per evitare di prestare occasione ai malintenzionati.
È con questo obiettivo che, in questa newsletter, vengono offerti dei consigli particolarmente interessanti ed efficaci.

Nicola Gori

AL PRIMO POSTO LA SICUREZZA

Il Governatorato dello Stato della Città del Vaticano ha sempre collocato al primo posto la sicurezza e la protezione dei propri sistemi informatici. Questo è un impegno che ha contraddistinto la nascita e lo sviluppo della rete internet all'interno dello Stato e dei suoi sistemi operativi.

D'altra parte, le risorse impiegate nella cybersicurezza non sono indifferenti, perché mirano a proteggere e tutelare, in primo luogo, l'immagine del Pontefice, e il quotidiano utilizzo dei dispositivi da parte dello Stato al suo servizio.

È in questo senso che, la Direzione dei Servizi di Sicurezza e Protezione Civile del Governatorato, il 18 luglio 2024, ha siglato un Protocollo d'intesa con l'Agenzia per la cybersicurezza nazionale della Repubblica Italiana (Acn).

L'obiettivo è stato lo scambio informativo, le attività di formazione e i progetti di cybersicurezza per incrementare le capacità e le competenze tecniche e scientifiche, in materia di prevenzione del rischio legato alla criminalità nel cyberspazio.

Si è trattato di un passo importante per assicurare una maggiore cooperazione nell'elaborazione di programmi formativi nell'ambito della cybersicurezza.

Con un'attenzione privilegiata allo scambio di informazioni, esperienze e procedure in questo settore, volte a garantire la tutela dello spazio cibernetico, promuovendo anche progetti di ricerca per il potenziamento delle capacità e delle competenze tecniche e scientifiche.

È evidente che, questo Protocollo d'intesa, è solo una parte dello sforzo del Governatorato per assicurare a tutte le sue realtà i cardini della sicurezza informatica: difesa perimetrale, sicurezza delle informazioni, gestione delle identità e degli accessi (Iam), integrità dei dati e disponibilità.

Nonostante il forte investimento nella cybersicurezza, c'è bisogno non solo di sistemi operativi e di tecnologia, ma della collaborazione di tutti quanto fanno parte della comunità lavorativa del Governatorato. È ciò che fa la differenza e permette di assicurare un livello più elevato di protezione.

Pertanto, questa newsletter vuole essere un'occasione per apprendere e memorizzare delle buone pratiche, che impediscano di offrire uno spazio, in cui i criminali possono inserirsi.

È con questo auspicio che auguro una buona lettura.

Sr. Raffaella Petrini
Presidente del Governatorato dello Stato della Città del Vaticano

CYBER SECURITY: UNA VISIONE STRATEGICA TRA TECNOLOGIA, RESILIENZA E CULTURA DELLA SICUREZZA

In un mondo sempre più interconnesso, in cui la digitalizzazione permea ogni ambito, la cyber security non è più una questione tecnica limitata ai Servizi IT, ma rappresenta una delle principali sfide strategiche per la protezione di servizi, dati ed asset. Le minacce cyber, con la loro capacità di colpire velocemente, su vasta scala e con impatti trasversali, richiedono sempre più una risposta sistemica e continua.

Nel contesto attuale, si è chiamati a sviluppare una visione strategica a lungo termine per la protezione del proprio spazio digitale. Tale visione deve fondarsi su tre pilastri fondamentali:

- Infrastrutture e processi sicuri,
- competenze tecniche evolute;
- una cultura della sicurezza diffusa.

L'analisi della situazione attuale mostra che le infrastrutture digitali – reti, data center, piattaforme – sono oggi strutturate per garantire robustezza, continuità operativa e affidabilità, pur in un contesto di contenimento dei costi. Tuttavia, la rapida evoluzione delle tecnologie e l'aumento esponenziale delle minacce richiedono un modello di evoluzione continua. Non si tratta solo di aggiornare hardware e software, ma di trasformare l'intero sistema in una infrastruttura adattiva e intelligente, capace di apprendere dai dati e reagire in tempo reale. In questo senso, l'adozione di modelli di zero trust architecture, la virtualizzazione dei sistemi e l'integrazione dell'intelligenza artificiale nei meccanismi di rilevamento rappresentano elementi chiave per una difesa avanzata.

Tradizionalmente, la sicurezza informatica si è concentrata sulla protezione del perimetro: firewall, antivirus, segmentazione delle reti. Oggi, questo approccio non è più sufficiente. Gli attacchi non si limitano a forzare le "porte di ingresso" ma sfruttano vulnerabilità interne, comportamenti umani e dispositivi connessi.

Una strategia moderna di cyber security deve quindi includere:

- Monitoraggio continuo e threat intelligence: la capacità di analizzare flussi di dati in tempo reale, identificare pattern anomali e anticipare i comportamenti malevoli.
- Incident response e resilienza operativa: predisporre piani strutturati di risposta agli incidenti e garantire la business continuity anche durante gli attacchi.

- Cyber deterrenza: rafforzare le capacità difensive per disincentivare gli attaccanti, anche attraverso cooperazioni internazionali e cyber diplomacy.
- Protezione end-to-end: garantire la sicurezza in ogni fase del ciclo di vita dei dati, dalla raccolta alla conservazione, fino alla distruzione.

Questo approccio implica una transizione dalla semplice difesa alla proattività: identificare, valutare e neutralizzare le minacce prima che si trasformino in incidenti.

Uno degli aspetti più sottovalutati, ma decisivi, della sicurezza informatica è il più volte citato fattore umano. Le statistiche confermano che una percentuale significativa degli attacchi informatici ha successo a causa di errori umani, disattenzioni o mancanza di consapevolezza. Per questo motivo, accanto all'innovazione tecnologica, è essenziale promuovere una cultura della sicurezza che coinvolga ogni livello dell'organizzazione, dai decisori di vertice fino agli utenti finali. In tale contesto, iniziative come: programmi di formazione continua a tutto il personale, campagne di consapevolezza sul phishing e social engineering, simulazioni di attacco, corsi su cyber hygiene, diventano strumenti fondamentali per creare un ecosistema sicuro.

Si possono ad esempio valorizzare i cinque fattori della cyber hy-

giene nella propria struttura lavorativa.

• Segmentazione. La rete dati va segmentata in aree circoscritte tali da garantire la protezione dell'intero sistema e rendere i punti di accesso non vulnerabili agli attacchi. Questo tipo di sicurezza tende a soddisfare la protezione anche nel caso di esigenze di lavoro da remoto. Se ci dovesse essere una violazione, la sicurezza intrinseca sarà in grado di contenerla senza compromettere il resto delle attività.

• Crittografia. Se i firewall ed i protocolli di accesso sono violati e le altre difese falliscono, la crittografia fa sì che tutti i dati critici che sono stati memorizzati siano effettivamente inutili una volta nelle mani dei cyber criminali. Se non si sa come decodificarli e metterli insieme, i dati criptati diventano un rompicapo difficile da risolvere. Una buona igiene informatica presuppone di crittografare i file ed i dati prima di condividerli. Lo stesso vale per la crittografia del traffico di rete, ove possibile.

• Autenticazione a doppio fattore. La sicurezza è sempre più spesso legata alla persona, riconoscimento facciale ed impronte digitali ne sono un esempio. Anche solo implementare un'autenticazione di base a due fattori può rivelarsi utile per bloccare una prima ondata di violazioni. Più l'autenticazione diventa personale, più le reti saranno sicure. Dopotutto, è molto più complicato rubare l'impronta del pollice piuttosto che un codice pin!

• Aggiornamento costante. I malware si evolvono diventando

sempre più sofisticati ed è necessario essere pronti a fronteggiarli con gli aggiornamenti che vengono rilasciati continuamente a tale scopo.

• Privilegio minimo. Anche se si ha piena fiducia nei confronti dei propri dipendenti non significa che tutti abbiano effettivamente bisogno degli stessi livelli di accesso. Un buon metodo di lavoro in sicurezza è concedere all'utenza del dipendente solo gli accessi di cui ha effettivamente bisogno. Riducendo al minimo l'accesso ai dati sensibili si vanno a limitare i punti di vulnerabilità.

Per concludere, guardando al futuro, il concetto da abbracciare non è solo la cyber security, ma la più ampia e ambiziosa cyber resilienza. Questo significa:

- prevedere l'imprevedibile,
- rispondere con flessibilità e rapidità agli eventi critici,
- ripristinare le funzioni in tempi certi,
- adattarsi e migliorare costantemente.

Nel cyberspazio, la resilienza è più importante dell'invulnerabilità.

La massima tutela si ottiene investendo nella costruzione di una identità cibernetica forte, basata su infrastrutture resilienti, persone consapevoli e un'azione strategica multilivello. Solo così sarà possibile affrontare le sfide della sicurezza digitale del presente e del futuro.

Ing. Antonino Intersimone
Direttore della Direzione delle Telecomunicazioni e dei Sistemi Informatici

10 REGOLE D'ORO PER ESSERE IN RETE IN SICUREZZA: COME PROTEGGERE LA TUA VITA DIGITALE DA MINACCE E TRUFFE

La sicurezza online è una delle principali preoccupazioni dell'era digitale. Proteggere i propri dati e la propria identità in rete è fondamentale per evitare truffe, furti di identità e attacchi informatici. Ecco **dieci regole essenziali** per navigare in sicurezza e ridurre i rischi.

1. Usare password forti e uniche e prediligere l'uso di passphrase

Secondo le linee guida del **National Institute of Standards and Technology (NIST)**, una password sicura deve avere almeno **12-16 caratteri**, includere **lettere maiuscole e minuscole**, **numeri e caratteri speciali** ed evitare parole di uso comune. È consigliabile utilizzare un **password manager** per generare e archiviare in modo sicuro le credenziali, evitando di riutilizzare la stessa password per più account.

Nel panorama della sicurezza informatica, l'adozione delle passphrase si rivela una scelta sempre più consigliata e auspicabile. A differenza delle tradizionali password, le passphrase rappresentano una stringa di parole più lunga e articolata, progettata per garantire un livello di protezione superiore nei processi di autenticazione.

Mentre le password convenzionali sono spesso limitate a una sequenza di massimo sedici caratteri, una passphrase può estendersi fino a cento caratteri o più. La sua struttura, basata su una combinazione di parole, punteggiatura e lettere maiuscole o minuscole, la rende estremamente resistente agli attacchi informatici, pur mantenendo un'elevata facilità di memorizzazione per l'utente.

L'utilizzo delle passphrase non solo rafforza la sicurezza contro accessi non autorizzati, ma migliora anche l'usabilità: a differenza delle complesse sequenze alfanumeriche delle password tradizionali, le passphrase si basano su frasi di senso compiuto, risultando più intuitive e meno soggette a dimenticanza.

Questa tipologia di autenticazione è ormai ampiamente impiegata in contesti che richiedono standard di sicurezza elevati, come la crittografia dei dati e la protezione di sistemi operativi

e applicazioni avanzate. Il crescente supporto per le passphrase da parte di molte piattaforme informatiche sottolinea la necessità di un'evoluzione nelle pratiche di protezione degli accessi digitali, ponendo l'accento su un equilibrio tra sicurezza e usabilità.

2. Attivare l'autenticazione multi-fattore (MFA)

L'autenticazione multi-fattore (MFA) aggiunge un ulteriore livello di sicurezza, richiedendo più di un metodo di verifica per accedere agli account. Oltre alla password, può includere codici OTP inviati via SMS o app di autenticazione, autenticazione biometrica o chiavi di sicurezza hardware, rendendo più difficile l'accesso non autorizzato. Il **NIST consiglia** di preferire l'uso di app **di autenticazione** o **chiavi fisiche** rispetto agli SMS, che possono essere intercettati.

3. Diffidare di email e messaggi sospetti (Phishing)

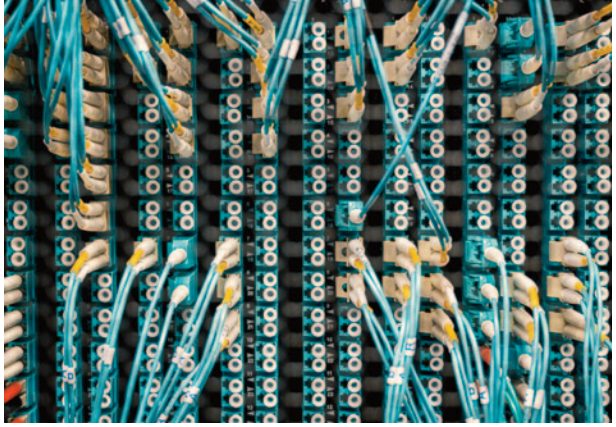
Le truffe di phishing mirano a sottrarre informazioni sensibili simulando comunicazioni ufficiali. È importante non cliccare su link sospetti e verificare sempre la fonte del messaggio prima di inserire dati personali o bancari. Secondo il **Centro Nazionale per la Cybersecurity (NCSC)**, più del 90% degli **attacchi informatici** inizia con un'email di phishing.

4. Aggiornare regolarmente i dispositivi e i software
Gli aggiornamenti di sistema e delle applicazioni contengono spesso **correzioni di sicurezza** per proteggere i dispositivi da vulnerabilità note. Attivare gli aggiornamenti automatici è un'ottima pratica. Il **NIST** e altre organizzazioni di sicurezza raccomandano di applicare immediatamente le patch di sicurezza rilasciate per evitare attacchi basati su exploit noti.

5. Proteggere i dati sensibili e la privacy
Evitare di condividere informazioni personali o finanziarie su siti non sicuri e limitare la quantità di dati pubblicati sui social media. È consigliabile rivedere le impostazioni della privacy per controllare chi può visualizzare i propri contenuti. Il **Regolamento Generale sulla Protezione dei Dati (GDPR)** sottolinea l'importanza di proteggere i dati personali per prevenire utilizzi impropri.

6. Verificare la sicurezza dei siti web
Prima di inserire dati sensibili su un sito web, assicurarsi che utilizzi il protocollo **HTTPS** e che il certificato SSL sia valido. I siti affidabili mostrano un'icona di lucchetto accanto all'indirizzo nella barra del browser. Secondo il **Google Transparency Report**, i siti che non utilizzano HTTPS sono più esposti a intercettazioni e attacchi man-in-the-middle.

7. Evitare connessioni Wi-Fi pubbliche non protette



Le reti Wi-Fi aperte sono spesso vulnerabili agli attacchi. Se è necessario utilizzarle, è consigliabile navigare solo su siti sicuri e impiegare una **VPN (Virtual Private Network)** per proteggere i dati trasmessi. Il **Federal Bureau of Investigation (FBI)** consiglia di evitare l'accesso a conti bancari o dati sensibili tramite Wi-Fi pubblico senza protezione.

8. Fare attenzione agli allegati e ai download
File e programmi scaricati da fonti non attendibili possono contenere malware. È buona norma verificare la provenienza dei file prima di aprirli e utilizzare un **antivirus aggiornato**. Secondo il **Cybersecurity and Infrastructure Security Agency (CISA)**, gli allegati in formato .exe, .zip e .js sono tra i più comuni veicoli di malware.

9. Controllare regolarmente i propri account
Monitorare l'attività degli account online per individuare accessi sospetti. Servizi come **"Have I Been Pwned"** consentono di verificare se le proprie credenziali siano state compromesse in violazioni di dati. Il **NCSC** suggerisce di attivare notifiche per accessi non riconosciuti e modificare immediatamente le password in caso di sospette violazioni.

10. Usare strumenti di sicurezza affidabili
L'uso di un **antivirus aggiornato**, un **firewall** attivo e una **VPN** aiuta a proteggere i dati da malware e accessi non autorizzati. È importante scegliere strumenti di sicurezza affidabili e di produttori riconosciuti. Il **NIST** raccomanda di abilitare sempre le funzioni di sicurezza integrate nei sistemi operativi, come il firewall e il controllo degli accessi.

Conclusione
Seguire queste dieci regole aiuta a **ridurre il rischio di attacchi informatici** e a mantenere al sicuro la propria identità digitale. La consapevolezza e la prudenza sono le migliori difese contro le minacce della rete. Implementare queste pratiche, offre una protezione efficace contro le minacce digitali.

Emmanuele Valeri

RANSOMWARE: L'ULTIMA FRONTIERA DELLE ESTORSIONI DIGITALI E COME DIFENDERSI

Accendere il proprio computer una mattina e trovarsi di fronte un messaggio inquietante sullo schermo:
"I tuoi file sono stati criptati. Per riaverli, paga un riscatto in criptovaluta entro 72 ore!"
Questo scenario drammatico è la realtà che molte aziende e privati affrontano quotidianamente a causa dei ransomware: una delle minacce più devastanti nel panorama della sicurezza informatica.

Cosa sono i ransomware?
I ransomware (ransom dal francese antico ranson=riscatto, e ware abbr. di software) sono una forma di malware progettata per bloccare l'accesso ai dati di un sistema attraverso la crittografia. Gli aggressori chiedono poi un riscatto, solitamente in criptovalute come Bitcoin, Ethereum o altro, in cambio della chiave di decrittazione necessaria per recuperare i file.
Esistono due tipi principali di ransomware:
- **Locker Ransomware:** Blocca l'accesso all'intero dispositivo, rendendolo inutilizzabile.
- **Crypto Ransomware:** Cifra file specifici, come documenti, immagini e database, lasciando il sistema operativo funzionante per consentire la comunicazione con gli aggressori.

Come Avvengono gli Attacchi?
Gli attacchi ransomware si diffondono attraverso diverse tecniche, tra cui:
- **E-mail di Phishing:** Gli aggressori inviano e-mail che sembrano provenire da fonti affidabili. Queste e-mail contengono link o allegati infetti che, una volta cliccati o aperti, installano il ransomware sul dispositivo della vittima.
- **Download da Siti Web Compromessi:** Visitare siti web non sicuri o scaricare software da fonti non affidabili può esporre a malware nascosti.
- **Vulnerabilità nei Sistemi:** Gli hacker sfruttano falle di sicurezza nei software o nei sistemi operativi per introdurre il ransomware. Questo è particolarmente comune quando non vengono applicati aggiornamenti e patch.
- **Dispositivi USB Infetti:** Anche i supporti fisici, come chiavette USB, possono essere utilizzati per diffondere ransomware.
- **Attacchi Mirati:** Le aziende più grandi sono spesso bersaglio di attacchi mirati, dove gli aggressori studiano la rete e cercano punti deboli prima di colpire.

Perché i Ransomware Sono Così Pericolosi?
Il ransomware è pericoloso per vari motivi:
- **Perdita di Dati:** Senza backup adeguati, i dati criptati possono essere irrecuperabili.
- **Impatto Economico:** Il pagamento del riscatto, i costi di ripristino ed il downtime possono comportare perdite finanziarie ingenti.
- **Danni Reputazionali:** Per le aziende, un attacco ransomware può minare la fiducia dei clienti e partner.

- **Evoluzione Costante:** I ransomware diventano sempre più sofisticati, rendendo difficile prevenirli.

Come Difendersi dai Ransomware

La prevenzione è la chiave per proteggersi da questa minaccia. Ecco alcune strategie efficaci per ridurre il rischio di un attacco ransomware:

- **Backup Regolari:** Salvare regolarmente i dati su dispositivi esterni o su servizi cloud sicuri. Assicurarsi che i backup siano isolati dalla rete principale per evitare che vengano colpiti durante un attacco.
- **Aggiornamenti e Patch:** Tenere sempre aggiornati il sistema operativo e i software utilizzati. Molti ransomware sfruttano vulnerabilità note che possono essere risolte con patch tempestive.
- **Formazione del Personale:** Per le aziende, è fondamentale educare i dipendenti a riconoscere e-mail sospette e altre tecniche di social engineering. Una formazione regolare può prevenire errori umani.
- **Soluzioni di Sicurezza Avanzate:** Utilizzare software antivirus, firewall e sistemi di rilevamento delle intrusioni per monitorare e bloccare attività sospette. Molti strumenti includono anche protezioni specifiche contro i ransomware.
- **Autenticazione a Due Fattori (2FA):** Proteggere gli account con l'autenticazione a due fattori per rendere più difficile agli hacker l'accesso ai sistemi aziendali.
- **Accesso Limitato:** Applicare il principio del privilegio minimo, concedendo ai dipendenti l'accesso solo alle risorse necessarie per il loro lavoro. Questo limita i danni potenziali in caso di attacco.
- **Monitoraggio e Audit Periodici:** Per le aziende, effettuare controlli regolari sulla sicurezza dei sistemi può aiutare a identificare vulnerabilità prima che vengano sfruttate.
- **Piani di Risposta agli Incidenti:** Preparare un piano dettagliato su come rispondere a un attacco ransomware. Questo dovrebbe includere istruzioni su come isolare i sistemi infetti, comunicare con le parti interessate e avviare il recupero dei dati.

Cosa Fare in Caso di Attacco

In caso di un attacco di tipo ransomware, è fondamentale agire tempestivamente:

- **Isolare i Sistemi Infetti:** Scollegare immediatamente i dispositivi colpiti dalla rete per evitare la propagazione del malware.
- **Mai Pagare il Riscatto!!!:** Pagare non garantisce il recupero dei dati coinvolti, inoltre contribuisce al finanziamento di ulteriori attacchi.
- **Contattate le Autorità:** Segnalare l'incidente alle forze dell'ordine o altri enti competenti.
- **Consultate Esperti di Cybersecurity:** Specialisti del settore possono aiutare a mitigare i danni e a trovare soluzioni per ripristinare i sistemi (ad es.: https://www.nomoreransom.org).

Conclusione

I ransomware rappresentano una delle minacce a maggior impatto nell'era digitale, ma con le giuste precauzioni è possibile ridurre drasticamente il rischio di essere colpiti: investire nella formazione di tutto il personale su tematiche quali la sicurezza delle informazioni, investire nella tecnologia e nella ricerca di personale specializzato in cybersicurezza sono oggi essenziali per proteggere le aziende e le persone. La sicurezza informatica non è da considerarsi come un lusso, ma è una necessità fondamentale in un mondo sempre più connesso.

Gabriele Pozzoli

CYBER SECURITY E SMART HOME: LA SICUREZZA DEI DISPOSITIVI CONNESSI E LE NUOVE MINACCE PER LA PRIVACY

Introduzione
La crescente diffusione della tecnologia nelle abitazioni ha trasformato radicalmente il modo in cui interagiamo con il nostro ambiente domestico. Dagli elettrodomestici connessi ai sistemi di sicurezza avanzati, il concetto di "smart home" ha reso le nostre case più efficienti e confortevoli. Tuttavia, l'integrazione di questi dispositivi introduce nuove problematiche di sicurezza informatica e privacy che non possono essere ignorate.

La vulnerabilità dei dispositivi IoT
Uno dei principali rischi riguarda la vulnerabilità dei dispositivi IoT (Internet of Things). A differenza di computer e smartphone, spesso dotati di robuste misure di sicurezza, molti dispositivi domestici intelligenti vengono progettati con standard di protezione minimi. Questo li rende facili bersagli per gli hacker, che possono accedere a telecamere di sorveglianza, termostati e assistenti vocali per compromettere la sicurezza della casa e la privacy degli utenti. Una volta violato un dispositivo, un attaccante potrebbe utilizzarlo per monitorare le attività domestiche, raccogliere informazioni sensibili o addirittura prendere il controllo di altri dispositivi connessi alla rete.

La scarsa consapevolezza degli utenti
Un altro aspetto critico è la consapevolezza degli utenti in merito alla sicurezza informatica. Molti consumatori acquistano dispositivi smart senza conoscere i rischi associati. Spesso non modificano le credenziali di default o non aggiornano il software regolarmente, lasciando aperte porte di accesso agli hacker. La mancata attenzione a queste misure basilari aumenta il rischio di violazioni e intrusioni. Inoltre, il traffico di rete domestico raramente viene monitorato dagli utenti, il che rende difficile rilevare eventuali anomalie o attività sospette.

La protezione dei dati personali
Oltre agli attacchi diretti ai dispositivi, vi è una crescente preoccupazione per la protezione dei dati personali. I dispositivi smart raccolgono una quantità significativa di informazioni sugli utenti, dalle abitudini quotidiane ai dati biometrici. Se queste informazioni finiscono nelle mani sbagliate, possono essere utilizzate per furto d'identità, sorveglianza non autorizzata o addirittura per la creazione di profili dettagliati a fini pubblicitari. Alcuni produttori hanno politiche poco trasparenti sulla gestione dei dati, rendendo difficile per gli utenti sapere come e dove vengano archiviati.

Attacchi informatici su larga scala
Le minacce informatiche non si limitano ai singoli utenti, ma possono avere conseguenze su vasta scala. I cybercriminali possono sfruttare i dispositivi IoT per creare botnet, reti di dispositivi infettati che vengono utilizzate per attacchi su larga scala, come il Distributed Denial of Service (DDoS). Un esempio noto è l'attacco del botnet Mirai nel 2016, che ha sfruttato migliaia di dispositivi IoT vulnerabili per bloccare interi servizi online. Questo dimostra come una gestione inadeguata della sicurezza informatica nelle abitazioni possa avere ripercussioni anche a livello globale.

Soluzioni e responsabilità
Affrontare queste sfide richiede un impegno congiunto da parte di produttori, utenti e istituzioni. I produttori dovrebbero adottare standard di sicurezza più elevati, implementare crittografia avanzata e garantire aggiornamenti software automatici per correggere eventuali vulnerabilità. Gli utenti, dal canto loro, dovrebbero adottare pratiche di sicurezza di base, come modificare le password predefinite, attivare l'autenticazione a due fattori e monitorare regolarmente i dispositivi connessi.

Il ruolo delle normative
Sul fronte normativo, alcuni passi avanti sono stati fatti, con regolamentazioni che impongono standard minimi di sicurezza per i dispositivi IoT. L'Unione Europea, con il GDPR, ha posto un forte accento sulla protezione dei dati, ma la rapida evoluzione della tecnologia richiede aggiornamenti costanti delle normative per garantire una sicurezza adeguata. È fondamentale che le aziende siano ritenute responsabili della protezione dei dati degli utenti e che vengano adottate misure più rigide per prevenire possibili violazioni.

Conclusioni
In un'epoca in cui la tecnologia è sempre più presente nelle nostre vite, garantire la sicurezza dei dispositivi connessi deve essere una priorità. La smart home offre numerosi vantaggi in termini di automazione e comfort, ma senza adeguate misure di protezione, il rischio di compromissione è elevato. Solo attraverso un approccio consapevole e l'adozione di soluzioni di sicurezza avanzate sarà possibile sfruttare appieno i benefici della tecnologia senza compromettere la propria privacy e sicurezza digitale.

Andrea Tripoli

SOCIAL ENGINEERING: COME I CRIMINALI SFRUTTANO GLI UMANI PER PENETRARE I SISTEMI

Una giornata di lavoro tipo... riceviamo una telefonata urgente da una persona che si presenta come un tecnico dell'ufficio informatico. In modo estremamente educato e gentile, ci informa che a causa di un problema critico con il nostro account occorre confermare alcune informazioni personali. Fornendo la password e successivamente il token di autenticazione, il tutto potrà essere risolto in sicurezza e senza perdite di tempo. Il tono rassicurante e pacato della conversazione potrebbe indurci a fidarci e collaborare, ma è proprio in situazioni come questa che i cybercriminali colpiscono. Questo è un classico esempio di social engineering.

Cos'è il Social Engineering?

Il social engineering è l'arte di manipolare le persone per ottenere accesso a informazioni o sistemi protetti: invece di cercare di violare complessi sistemi di sicurezza informatica, i criminali si concentrano su di un target di natura non tecnologica: l'essere umano. I cybercriminali sfruttano elementi quali la fiducia, la paura, la curiosità o l'urgenza delle loro vittime per indurle a compiere azioni dannose, come cliccare su un link sospetto, scaricare un file infetto o rivelare credenziali riservate.

Alcune delle Tecniche Più Comuni di Social Engineering:

1. **Phishing**

Il phishing è probabilmente la tecnica di social engineering più diffusa. Si manifesta attraverso e-mail, messaggi o persino chiamate telefoniche (cd. vishing: voice phishing) che sembrano provenire da fonti affidabili. I criminali cercano di ingannare la vittima spingendola a fornire informazioni sensibili o a scaricare malware.

2. **Pretexting**

In questo caso, l'attaccante si costruisce un pretesto, ovvero una storia credibile, per guadagnare la fiducia della vittima. Ad esempio, potrebbe fingere di essere un dipendente del reparto risorse umane o un fornitore di servizi.

3. **Baiting**

Il baiting sfrutta la curiosità delle persone. Un esempio classico è quello di una chiavetta USB lasciata intenzionalmente in un luogo pubblico magari con un'etichetta accattivante, come "Salari aziendali". Una volta collegato il device al computer, il malware infetta il sistema.

4. **Tailgating**

Questa tecnica avviene nel mondo fisico. Un criminale si infiltra in un edificio protetto semplicemente seguendo qualcuno che ha accesso, magari fingendo di aver dimenticato il badge.

Perché il Social Engineering è Così Efficace?

Il successo del social engineering si basa su alcuni fattori di natura psicologica:

- **Fiducia**: Le persone tendono a fidarsi di chi si presenta in modo professionale o autorevole.
- **Urgenza**: La pressione del tempo porta spesso le vittime a prendere decisioni impulsive.
- **Emozioni**: La paura o la curiosità possono spingere le persone ad agire senza riflettere.

Come Proteggersi?

Proteggersi dal social engineering richiede un mix di attenzione, buone abitudini e strumenti di sicurezza. Ecco alcuni consigli pratici, con un focus sul contesto lavorativo:

1. **Formazione Continua**

La consapevolezza è il primo passo. Partecipare regolarmente a corsi di formazione sulla sicurezza informatica può fare la diffe-

renza. Non devono essere lezioni complicate: anche semplici sessioni di aggiornamento su come riconoscere le tecniche di social engineering possono aiutare. Inoltre, simulare periodicamente attacchi (come falsi tentativi di phishing) può mettere alla prova il livello di preparazione del personale.

2. **Politiche di Verifica Rigide**

Mai fornire informazioni sensibili a chiunque avvii un contatto senza preavviso, anche se sembra una richiesta legittima. Prima di agire, meglio prendere un momento per verificare l'identità del richiedente. Ad esempio, se un "tecnico IT" chiede una password, potrebbe essere utile chiamare direttamente il reparto IT utilizzando un numero di telefono ufficiale, invece di quello fornito dal presunto tecnico.

3. **Cultura della Sicurezza**

È fondamentale creare un ambiente di lavoro in cui tutti si sentano responsabili della sicurezza. Promuovere la segnalazione di comportamenti o richieste sospette. Nessuno dovrebbe sentirsi a disagio nel dire "questa richiesta sembra strana" o nel chiedere una seconda opinione.

4. **Protezione dei Dispositivi**

Mai lasciare laptop, smartphone o dispositivi aziendali incustoditi, soprattutto in spazi condivisi o pubblici. Utilizzare blocchi schermo con password o codici PIN e assicurarsi che i dispositivi si blocchino automaticamente dopo un periodo di inattività.

5. **Autenticazione a Due Fattori (2FA)**

Anche se qualcuno riesce a ottenere una password di accesso, l'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza. Questo strumento, che richiede un secondo passaggio per confermare l'identità dell'utente, è essenziale per proteggere account aziendali.

6. **Accesso Fisico Controllato**

Assicurarsi che solo le persone autorizzate possano accedere agli uffici o alle aree sensibili. Sistemi come badge personali, telecamere di sorveglianza e porte con serrature elettroniche sono strumenti efficaci per prevenire intrusioni fisiche.

7. **Attenzione ai Segnali di Allarme**

Fare attenzione ai dettagli. E-mail con errori grammaticali, richieste inusuali o mittenti sconosciuti sono spesso segnali di pericolo. Prima di cliccare su un link o scaricare un allegato, chiedersi sempre se la richiesta ha senso. In caso di dubbi, è meglio non rischiare.

8. **Test e Audit Periodici**

Effettuare regolarmente audit di sicurezza e test di penetrazione per individuare eventuali vulnerabilità nei sistemi e nei processi. Questi test possono rivelare punti deboli che altrimenti potrebbero essere sfruttati dai cybercriminali.

Conclusione

Il social engineering è una minaccia insidiosa, ma non invincibile. Essere consapevoli di come i criminali operano e adottare buone pratiche può ridurre notevolmente i rischi. Sul posto di lavoro, investire nella formazione dei dipendenti, promuovere una cultura della sicurezza e utilizzare strumenti adeguati sono passi fondamentali per proteggere informazioni sensibili e sistemi critici. Spesso la sicurezza non dipende solo dalla tecnologia, ma da quanto noi esseri umani siamo attenti e preparati a riconoscere le trappole.

G. P.

MINACCE INVISIBILI: LA CRESCITA DEGLI ATTACCHI CIBERNETICI

Introduzione
Nell'era digitale, le minacce cibernetiche sono diventate un pericolo sempre più sofisticato e difficile da rilevare. Le organizzazioni di ogni settore devono affrontare attacchi che mirano ai dati sensibili, alla continuità operativa e alla reputazione aziendale. La crescita di questi attacchi comporta non solo danni economici diretti, ma anche perdite di fiducia da parte di clienti e partner. Questo articolo analizza le principali minacce informatiche, le sfide economiche che pongono alle aziende e le strategie per difendersi efficacemente.

1. Le Principali Minacce Cibernetiche
Gli attacchi informatici si evolvono continuamente e sfruttano vulnerabilità sia tecnologiche che umane. Tra le minacce più diffuse troviamo:
- **Ransomware**: Malware che crittografa i dati aziendali, bloccandone l'accesso fino alla richiesta di pagamento di un riscatto.
- **Phishing e Spear Phishing**: Email fraudolente che mirano a sottrarre credenziali e dati sensibili tramite social engineering.
- **Attacchi Zero-Day**: Sfruttano vulnerabilità non ancora note presenti nei software, con l'obiettivo di colpire la vittima prima che vengano corrette dai produttori.
- **Malware e Trojan**: Programmi dannosi che si infiltrano nei sistemi per rubare informazioni o consentire accessi non autorizzati.
- **Denial of Service (DoS) e Distributed Denial of Service (DDoS)**: Attacchi che sovraccaricano i server aziendali, rendendoli inaccessibili agli utenti legittimi.
- **Furto di Credenziali e Violazioni di Dati**: Tecniche di attacco che compromettono le credenziali aziendali per accedere a sistemi riservati.

2. Le Sfide Economiche per le Organizzazioni
Gli attacchi cibernetici non si limitano a compromettere i sistemi IT, ma hanno un impatto economico significativo. Tra le principali conseguenze vi sono:
- **Costi di ripristino**: Le aziende colpite devono investire in analisi forensi, ripristino dei dati e potenziamento delle misure di sicurezza.
- **Sanzioni e cause legali**: Normative come il GDPR prevedono pesanti sanzioni in caso di violazione dei dati personali.

- **Danni alla reputazione**: La perdita di fiducia da parte di clienti e partner può ridurre drasticamente il valore del brand.
- **Interruzione operativa**: Un attacco riuscito può bloccare le operazioni aziendali per giorni o settimane, con perdite economiche elevate.

3. Strategie di Difesa e Soluzioni
Per mitigare i rischi, le organizzazioni devono adottare una strategia di cybersecurity proattiva. Ecco alcune misure chiave:
- **Formazione e sensibilizzazione**: Educare i dipendenti sulle minacce informatiche riduce il rischio di attacchi basati sull'inganno umano.
- **Implementazione della Multi-Factor Authentication (MFA):** Aggiungere un ulteriore livello di sicurezza agli accessi riduce il rischio di compromissione degli account.
- **Aggiornamenti e patch di sicurezza**: Mantenere sempre aggiornati software e sistemi operativi per proteggersi dagli exploit.
- **Backup regolari e crittografati**: Eseguire backup frequenti e conservarli in luoghi sicuri per garantire un ripristino rapido in caso di attacco.
- **Monitoraggio continuo e threat intelligence**: Utilizzare strumenti avanzati di rilevamento delle minacce per individuare e rispondere rapidamente a comportamenti sospetti.
- **Firewall e sistemi di prevenzione delle intrusioni (IDS/IPS):** Proteggere la rete aziendale da accessi non autorizzati e attacchi esterni.
- **Zero Trust Architecture**: Adottare un modello di sicurezza che non considera attendibile nessun accesso, richiedendo verifiche costanti per ogni transazione di dati.

Conclusione
Gli attacchi informatici rappresentano una minaccia in continua evoluzione, con impatti significativi sulle aziende sia in termini di sicurezza che di costi economici. Adottare un approccio proattivo alla cybersecurity, investire nella protezione dei dati e formare il personale sono passi essenziali per difendersi dalle minacce invisibili del mondo digitale. Solo con una strategia integrata e una costante vigilanza è possibile proteggere efficacemente le infrastrutture aziendali e garantire la resilienza operativa.

E. V.

CYBER SECURITY NEI GOVERNI: MINACCE GLOBALI E STRATEGIE DI DIFESA

Negli ultimi anni, la digitalizzazione ha trasformato il modo in cui i governi operano, introducendo nuove opportunità ma anche nuove vulnerabilità. La sicurezza informatica è diventata un pilastro essenziale per la stabilità nazionale, con le amministrazioni pubbliche che si trovano a fronteggiare attacchi sempre più sofisticati e mirati. La gestione di dati sensibili, il controllo delle infrastrutture critiche e l'erogazione di servizi essenziali rendono gli enti governativi bersagli di cyber attacchi con implicazioni geopolitiche, economiche e sociali.

Il costo degli attacchi informatici nel settore pubblico continua a crescere, con studi che evidenziano un impatto finanziario pari a miliardi di dollari ogni anno. Un dato emblematico è il caso del servizio sanitario irlandese, paralizzato da un attacco ransomware nel 2023 che ha causato danni superiori ai cento milioni di euro. Incidenti di questa portata non si limitano a una questione economica, ma sollevano problemi di fiducia e di sicurezza pubblica. Quando le informazioni personali dei cittadini vengono compromesse, la percezione di vulnerabilità si diffonde rapidamente, minando il rapporto tra lo Stato e i suoi cittadini.

La reputazione di un governo può essere gravemente compromessa da una violazione della sicurezza informatica. Nel 2020, un attacco ai sistemi sanitari norvegesi ha esposto dati personali di quasi tre milioni di cittadini, riducendo drasticamente l'adesione ai servizi digitali pubblici. Il timore che i dati personali possano essere sottratti o manipolati frena l'innovazione e ostacola l'adozione di tecnologie digitali, con ripercussioni dirette sulla modernizzazione della pubblica amministrazione e di qualsiasi organizzazione governativa.

Le strategie di difesa richiedono un approccio multilivello, in cui la prevenzione e la risposta agli incidenti giocano un ruolo cruciale. Molti sistemi utilizzati dagli enti governativi sono tecnologicamente obsoleti, un fattore che amplifica il rischio di attacco. La modernizzazione dell'infrastruttura IT deve diventare una priorità, accompagnata da politiche di sicurezza rigorose e dalla formazione continua del personale. L'errore umano resta infatti una delle principali cause di attacco informatico, rendendo indispensabili programmi di sensibilizzazione e simulazioni di attacco per migliorare la capacità di risposta alle minacce.

La sicurezza informatica non è solo un problema tecnico, ma una questione di sicurezza nazionale. Gli attacchi a infrastrutture critiche possono avere effetti devastanti, come dimostrato dal caso del Colonial Pipeline negli Stati Uniti, dove un attacco informatico ha interrotto la fornitura di carburante in intere regioni. La cooperazione internazionale è fondamentale per contrastare le minacce su larga scala, poiché i cyber criminali operano senza confini. La condivisione di informazioni tra governi e agenzie di sicurezza consente di anticipare le minacce e di migliorare la resilienza complessiva.

Il panorama della cyber security governativa è in continua evoluzione, con minacce che si adattano rapidamente alle nuove

misure di difesa. Investire nella protezione dei dati e delle infrastrutture critiche non è più un'opzione, ma una necessità imprescindibile per garantire la stabilità e la sicurezza delle istituzioni. In un mondo sempre più interconnesso, proteggere il cyberspazio equivale a proteggere la democrazia stessa.

Valerio Mercuri

GIOVANI PROTAGONISTI DELL'ETICA GLOBALE: CYBER DIPLOMACY, DIRITTO, ECONOMIA E TECNOLOGIA IN UN MONDO INTERCONNESSO

Come distinguere un fatto reale da un deepfake? Chi garantisce che un algoritmo non manipoli l'opinione pubblica? Queste domande hanno guidato il dibattito "Cyber Diplomacy, diritto, economia e tecnologia in un mondo interconnesso, AI e Futuro delle Istituzioni", organizzato dalla Direzione delle Telecomunicazioni e Servizi Informatici. Tra slide, dati e casi pratici, studenti e docenti hanno riflettuto su un tema cruciale: in un mondo iperconnesso, dove l'intelligenza artificiale (AI) può creare o distruggere verità in pochi click, l'etica e la conoscenza diventano l'unico antidoto alla disinformazione.

AI e post-verità: quando la tecnologia sfida la percezione
Il cuore del confronto è stato l'impatto giuridico/economico dei crimini informatici e il ruolo dell'AI nel plasmare la realtà. Da un lato, gli attacchi cyber non sono solo una minaccia tecnologica, ma un labirinto di sfide legali, costi economici esponenziali e rischi reputazionali. Dal punto di vista giuridico, i conflitti di giurisdizione (come il contrasto tra il GDPR europeo e il Cloud Act statunitense) rendono difficile perseguire i crimini digitali, mentre la mancanza di trattati internazionali vincolanti lascia spazio a zone grigie sfruttate da hacker e stati "canaglia".

Il costo economico è altrettanto critico: secondo stime recenti, il cybercrime costa all'economia globale 8.000 miliardi di dollari l'anno, cifra destinata a salire con l'avvento del quantum computing e degli attacchi alla supply chain. Incidenti come il ransomware al Colonial Pipeline (2021), che ha interrotto il flusso di carburante negli USA, hanno generato perdite dirette di 4,4 milioni di dollari, senza contare i danni indiretti alla fiducia dei consumatori.

Strumenti come i deepfake vocali o i video sintetici minacciano di erodere la fiducia nelle istituzioni: nel 2023, falsi audio attribuiti a politici hanno provocato volatilità nei mercati. Dall'altro, l'AI stessa può essere un'alleata: algoritmi di fact-checking e sistemi di rilevamento delle manipolazioni offrono speranze di controllo. «Il problema non è la tecnologia, ma come la usiamo». «Servono regole chiare: un deepfake per un film è creatività, per influenzare elezioni è un crimine».

Sapienza digitale: perché la conoscenza è un patrimonio da proteggere
Se i dati sono il "nuovo petrolio", la capacità di interpretarli è la vera ricchezza, proteggerli è il la grande sfida. Gli interventi hanno sottolineato come università e centri di ricerca debbano formare giovani non solo a programmare algoritmi, ma a interrogarsi sul loro impatto sociale.
Un esempio? Il GDPR europeo, che limita l'uso di dati sensibili, nasce da una visione etica: proteggere le persone, non solo i server. «La saggezza digitale è saper bilanciare innovazione e di-

ritti», il caso *Cambridge Analytica* esposto ha stigmatizzato il problema giuridico ancora acerbo, dove dati rubati hanno distorto campagne politiche e attacchi hacker sistemici e filo governativi hanno provocato impatti socio-economici drammatici.

Reputazione e cybersecurity: l'uomo al centro

La reputazione di uno Stato o di un'azienda oggi si gioca online. Attacchi come quello a *SolarWinds* (2020), che ha compromesso dati governativi USA, dimostrano che un malware può danneggiare più di un missile. Ma la soluzione non è solo tecnica: «Un firewall non ferma la manipolazione delle notizie». Servono "strategie olistiche":

- Piattaforme trasparenti che contrastino la disinformazione senza censurare;
- Educazione al pensiero critico, per riconoscere una fake news;
- Collaborazione e legislazione internazionale, sono le nuove frontiere su cui concentrarsi.

Il ruolo dei giovani: custodi di un futuro "umano"

In chiusura, l'appello ai nativi digitali: «Viviamo la prima generazione che può usare l'AI per amplificare la conoscenza, non per dividerla». Esempi concreti non mancano: startup guidate da under 30 sviluppano tool per verificare fonti giornalistiche, mentre altri progettano chatbot etici che rifiutano di generare discorsi d'odio.

L'evento ha lasciato messaggi semplici ma urgenti: in un'epoca in cui l'AI può rendere il falso più convincente del vero, difendere la verità è una responsabilità collettiva, la Cyber-Diplomacy è fondamentale per ridurre gli impatti Politico/Economici dagli effetti sociali potenzialmente devastanti.

E i giovani, con la loro familiarità tecnologica e sensibilità ai valori, sono chiamati a guidare questa battaglia silenziosa, regolamentarla e normalizzarla. Non con retoriche apocalittiche, ma con scelte quotidiane e tecnologiche: condividere una notizia solo dopo averla verificata, pretendere algoritmi trasparenti, difendere il sapere come bene comune. Perché, come ricorda un proverbio riletto in chiave digitale: La verità è come l'acqua: trova sempre la sua strada. Ma serve qualcuno che pulisca gli argini.

V. M.