Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Il perimetro cibernetico: approccio al rischio, analisi ed adeguamento dell'infrastruttura digitale e dei comportamenti, alla luce delle normative più recenti

a cura di Massimo Massimino
17 novembre 2022

anci Piemonte

Indice

- Il perimetro di sicurezza nazionale cibernetica
- Analisi del rischio
- Il comportamento
- Adeguamento dell'infrastruttura digitale

anci Piemonte

IFEL Fondazione ANCI

GLI ATTACCHI INFORMATICI ALLA PA SONO IN AUMENTO !!!

Negli scorsi mesi, molte PA sono state vittima di attacchi :

Alcuni esempi :
Comune di Brescia marzo 2021
Regione Lazio luglio 2021
Regione Lombardia ottobre 2021
Comune di Torino novembre 2021
ASL Città di Torino, agosto 2022

anci Piemonte

IFEL Fondazione ANCI

GLI ATTACCHI INFORMATICI ALLA PA SONO IN AUMENTO: I NUMERI DEL CSI PIEMONTE

I numeri del 2021

Numero di Server Protetti nel Data Center	455
Numero di URL dinamiche protette	317.334
Numero di Virtual Host protetti nel Data Center	922
Numero di eventi "malevoli" bloccati	Circa 14.500.000 (nella figura di dettaglio)

Rilevazione dei dati su un campione di 30 giorni

Alert Name	Severity	Num. of Events
Abnormally Long Header Line	High	31,023
Custom Violation	Low	34
Custom Violation	Medium	17,649
Custom Violation	High	54,847
Discrepancy between transfer-encoding and content-length	High	262
HTTP Signature Violation	Low	6,387
HTTP Signature Violation	High	418,963
Illegal Byte Code Character in Header Name	Medium	66,126
Illegal Byte Code Character in Header Value	Medium	8,660
Illegal Byte Code Character in Method	Medium	31,277
Illegal Byte Code Character in Parameter Name	Medium	524
Illegal Byte Code Character in Parameter Value	Medium	224
Illegal Byte Code Character in Query String	Medium	984
Illegal Byte Code Character in URL	Medium	22,600
Illegal HTTP Version	Medium	21,284
Illegal Host Name	Low	527
Illegal Parameter Encoding	Low	1,699
Illegal Response Code	Low	53
Illegal URL Path Encoding	Low	157,775
Malformed HTTP Header Line	High	38,704
Malformed URL	Low	36,506
NULL Character in Header Name	Low	54,211
NULL Character in Header Value	Low	7,708
NULL Character in Method	Low	27,935
NULL Character in Parameter Name	Low	694
NULL Character in Parameter Value	Low	8,392
NULL Character in Query String	Low	398
NULL Character in Url	Low	18,139
Redundant HTTP Headers	High	290
Redundant UTF-8 Encoding	Medium	3,729
SQL injection	High	13,381
Scraping Attack	Medium	13,550,803
Too Many Cookies in a Request	Low	9,968
Too Many Headers per Response	Medium	48,596
Too Many of the Same Response Code	Medium	38,396
Unauthorized Request Content Type	High	4,955
Unknown HTTP Request Method	Medium	35,526
Web Worm	High	8,284

DOMANDA 1

La prima parola che vi viene in mente se dico

CYBERSECURITY

Votate

Cos'è la cybersecurity

- Possiamo definire la cybersecurity (in italiano sicurezza informatica) come un insieme di mezzi, procedure e tecnologie atti alla protezione dei sistemi informatici.
- Vanno garantite Riservatezza, Integrità, Disponibilità (RID)
- Richiede costante impegno, individuale e organizzativo
- Senso di responsabilità
- La PA fa gola ai cyber criminali, per la grande quantità di dati, rivendibili sulla rete

Cos’è la cybersecurity

- Internet of Things, BYOD, Smart working aumentano il nostro benessere, ma possono diventare nuove via di attacco da parte dei cyber criminali.
- Le nostre abitudini e la nostra cybercultura possono essere decisivi nella salvaguardia della sicurezza nel posto di lavoro.
- Siamo nell’era dei big data : immense quantità di dati vengono scambiate ogni giorno e i tentativi di attacco sono in constante crescita

Formazione IFEL
per i Comuni

Il perimetro di sicurezza nazionale cibernetica

anci Piemonte

Il perimetro cibernetico

D.L. 105 del 21 settembre 2019

Il Perimetro di sicurezza nazionale cibernetica è volto a tutelare la sicurezza nazionale, mirando a un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici.

Si applica, pertanto, ai beni ICT che i soggetti inclusi nel Perimetro hanno individuato come necessari allo svolgimento di tali funzioni o servizi essenziali e che, in caso di incidente, causerebbero l'interruzione totale o una compromissione degli stessi con effetti irreversibili sotto il profilo dell'integrità o della riservatezza dei dati e delle informazioni.

I soggetti inclusi nel Perimetro sono Amministrazioni pubbliche, enti o operatori pubblici o privati, con sede nel territorio nazionale, che esercitano funzioni essenziali dello Stato

Il perimetro di sicurezza nazionale cibernetica: gli attacchi interni

- Il 20 % degli incidenti di sicurezza informatica provengono da attori interni all'organizzazione, sia per illeciti guadagni che per divertimento

- La componente psicologica del rapporto di lavoro

- Il modello organizzativo

Il perimetro di sicurezza nazionale cibernetica: gli hacker

- Un hacker cerca di modificare le funzionalità di un sistema, per fargli fare qualcosa di diverso

- Ha bisogno di competenze informatiche, ma sempre di più anche di tecniche di ingegneria sociale

Il framework nazionale per la Cybersecurity

- E’ lo strumento per analizzare e implementare le proprie misure di cybersecurity e si basa sul framework NIST, già adottato da numerosi altri paesi, a garanzia di uniformità
- Prevede 5 funzioni: Identify, Protect, Detect, Respond e Recover
- Le funzioni sono divise in categorie e sottocategorie, che rappresentano raccomandazioni che l’organizzazione può decidere di implementare
- L’insieme di sottocategorie scelte da un’organizzazione definiscono il profilo, definendo livelli di priorità nell’implementazione

https://www.cybersecurityframework.it/framework2

I controlli Essenziali di Cybersecurity

- 2016 Italian Cybersecurity Report: Controlli Essenziali di Cybersecurity
- Sono misure minime da implementare da parte di ogni organizzazione, e rappresentano un esempio di profilo del framework

https://www.cybersecurityframework.it/csr2016

L’approccio “ZERO-TRUST”

- approccio alla sicurezza IT che presuppone l'assenza di un perimetro di rete affidabile e in base al quale ogni transazione di rete deve essere autenticata prima che possa concretizzarsi.
- “Non fidarsi mai, verificare sempre !!”
- Eliminare la convinzione che qualsiasi elemento all'interno della rete sia sicuro. Non esiste più un perimetro sicuro, a causa dei cambiamenti lavorativi, dell'adozione di applicazioni basate su microservizi che possono avere componenti praticamente ovunque e della natura sempre più collaborativa dei processi aziendali.
- Non vi è più una divisione fra quello che è esterno alla azienda, quindi per definizione pericoloso, e quello che è interno e quindi, per ipotesi, non pericoloso.

Formazione IFEL
per i Comuni

Analisi del rischio

anci Piemonte

DOMANDA 2

Nel vostro Ente avete mai fatto formazione sui rischi cyber?

Votate

Analisi del rischio: 4 principi fondamentali

- La sicurezza è un processo
- La sicurezza di una catena è pari a quella del suo anello più debole
- Non si può gestire ciò che non si può misurare
- Non devi per forza essere un bersaglio per diventare una vittima

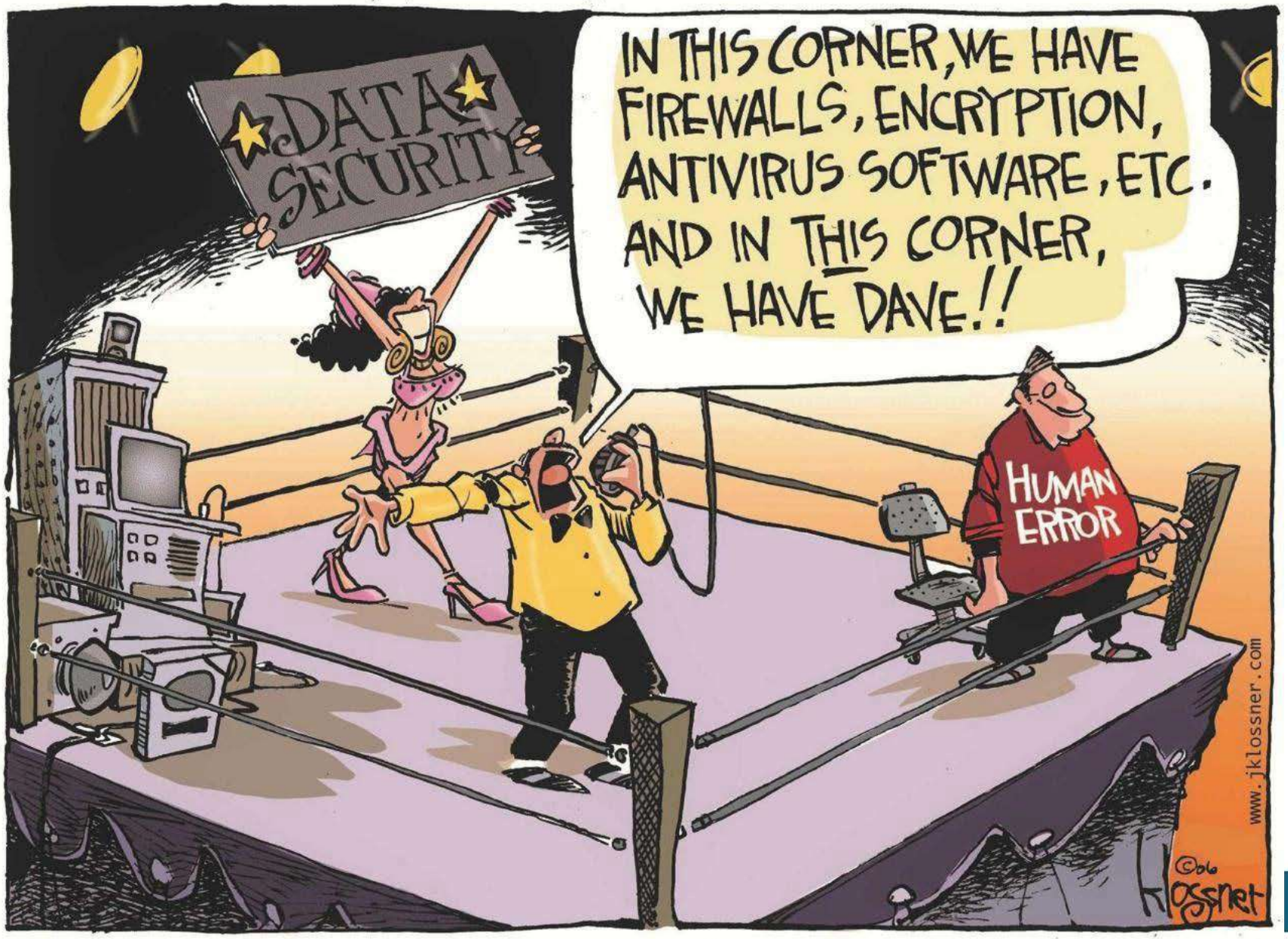
anci Piemonte

IFEL Fondazione ANCI

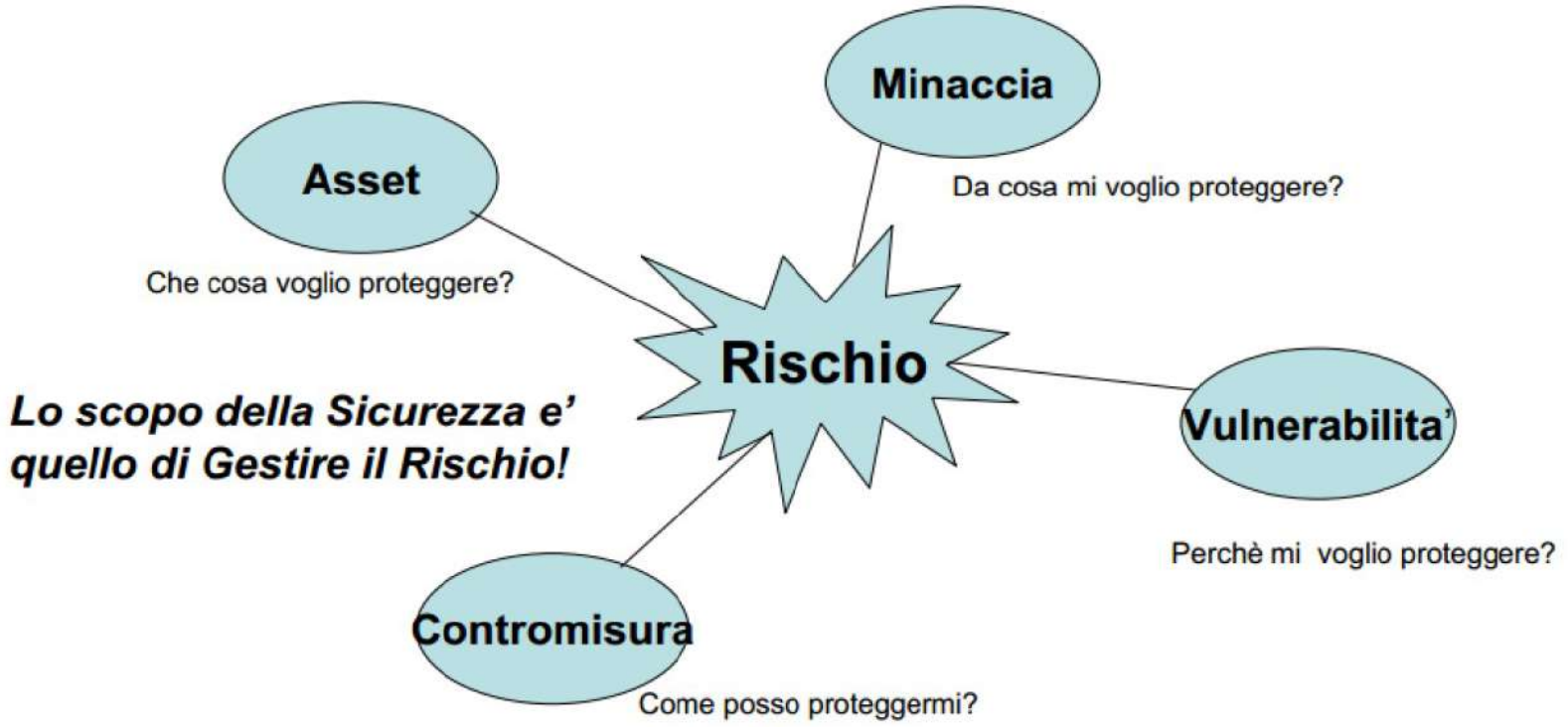
Le componenti del rischio

- Per una stima del rischio, occorre valutare adeguatamente una serie di elementi che rispondono tutti a domande ben precise

https://www.sicurezzait.gov.it/cyber/gestioneRischio.html


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©06 Klossner
www.jklossner.com

Cos’è la sicurezza?



Lo scopo della Sicurezza e’ quello di Gestire il Rischio!

Piemonte

Fondazione ANCI

Gestire il rischio

Il Risk Management si compone di 4 fasi

- **Identificazione**: si cerca di identificare le possibili fonti di rischio e individure i pericoli
- **Valutazione quantitativa e qualitativa**: deteminare impatto e probabilità di un pericolo e nell'assegnare un ordine di priorità dei rischi da affrontare
- **Pianificazione**: identificare l'insieme delle contromisure applicabili ad un certo rischio. Analisi costi/benefici e selezionare quelle da applicare
- **Controllo**: verificare se le contromisure applicate stanno funzionando e valutare l'insorgere di nuovi rischi

I risultati di ognuna delle fasi confluiscono nel piano del rischio complessivo

Il calcolo del rischio

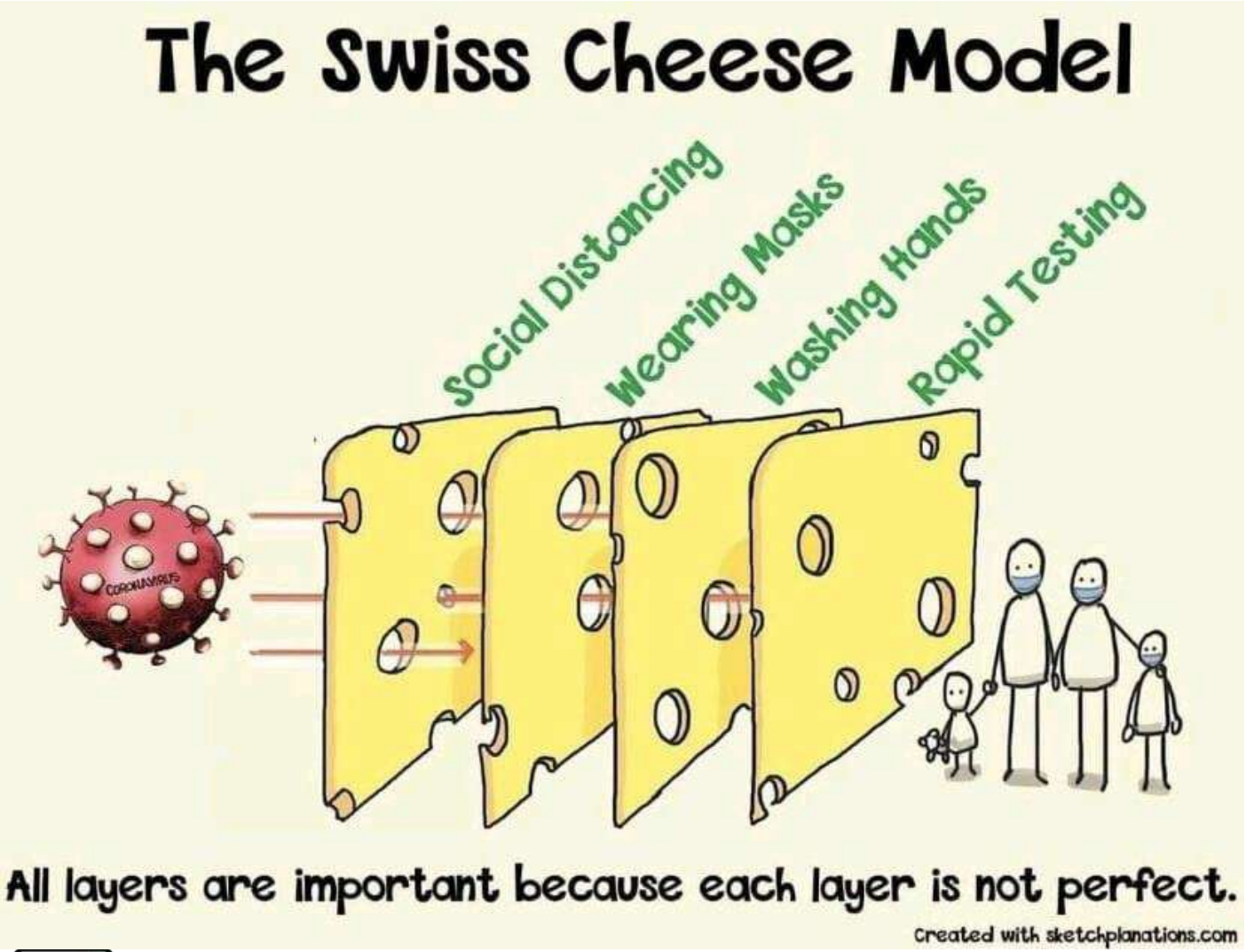
Il calcolo del rischio viene solitamente definito e calcolato come prodotto

R = P x I x E

P = Probabilità della minaccia (alto per minacce molto probabili

I = impatto (alto per danni consistenti)

E = Efficacia (alto per controlli poco efficaci)



Piemonte

Fondazione ANCI

Formazione IFEL
per i Comuni

Il comportamento

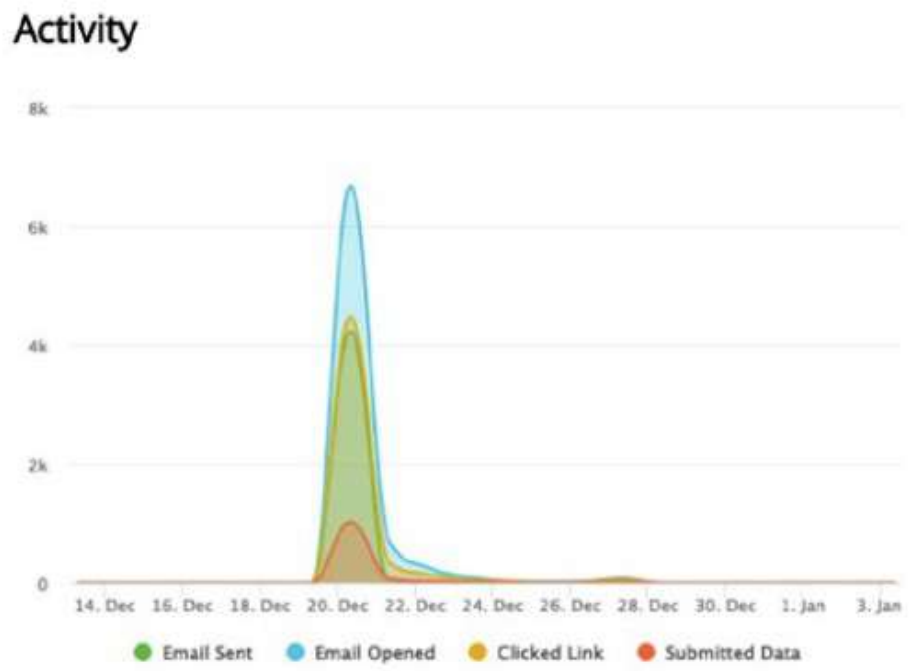
anci Piemonte

DOMANDA 3

Campagna di phishing simulato:
Ai dipendenti di un'azienda italiana è stata inviata una finta mail tecnica che chiedeva di inserire le proprie credenziali
Che percentuale ha abboccato, inviando le proprie credenziali?

Votate

Risultati



Overall Risk score	82%
Sent	4233
Opened	2836
Clicked	1295
Submitted	981
Reported	0

Figura 1 - *Campagna di phishing simulato (Fonte: servizio PhishBrain di Libraesva)*

Tratto dal Rapporto Clusit 2022 sulla sicurezza ICT in Italia

anci Piemonte

IFEL Fondazione ANCI

L’ingegneria sociale

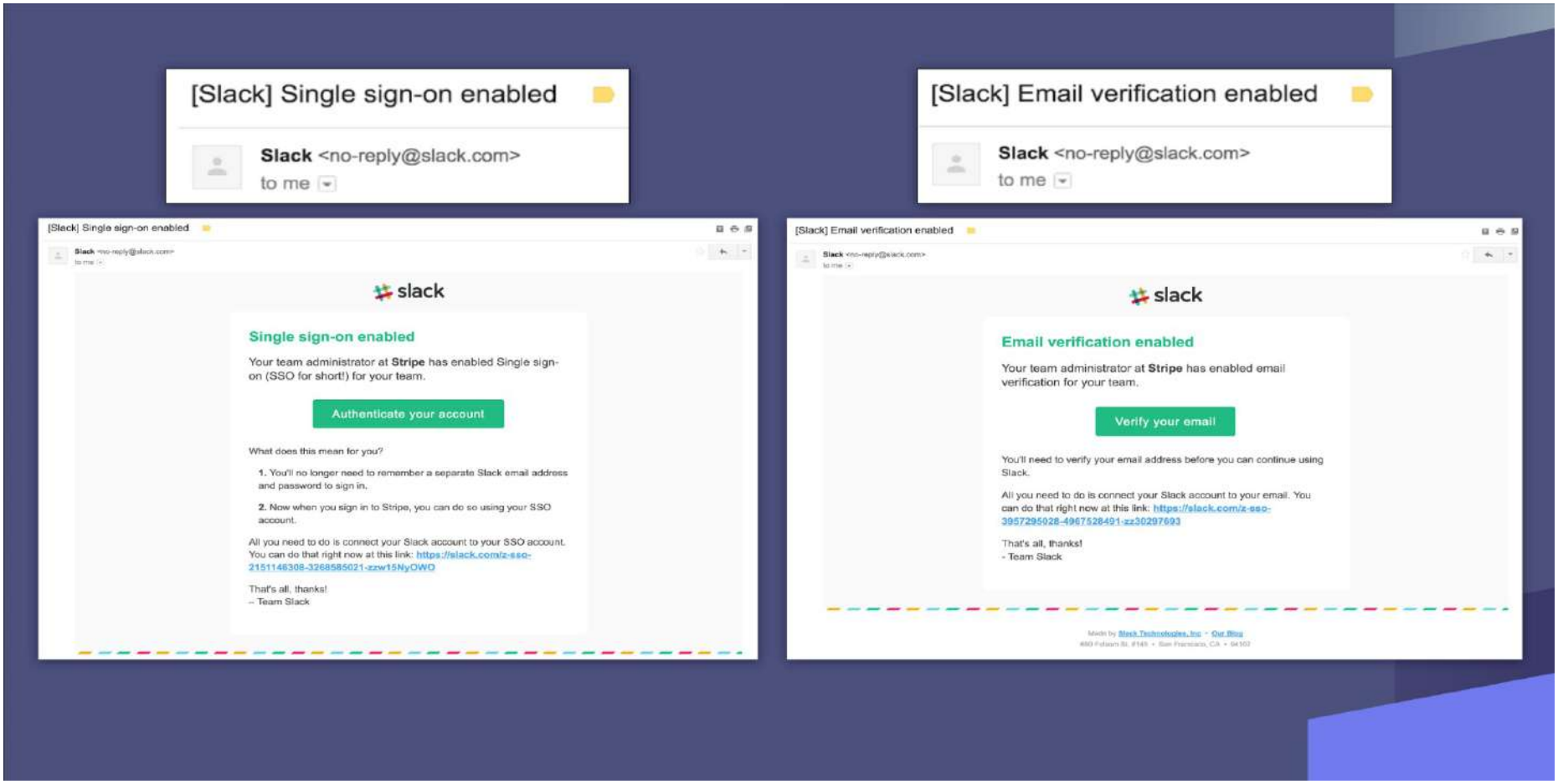
- L’ingegneria sociale ha come fine la manipolazione degli individui per far loro compiere azioni o convincerli a dare informazioni riservate

- Gli hacker investono molto in ingegneria sociale, perché è molto meno complicato compiere un attacco con il phishing rispetto ad attaccare un sistema protetto da firewall e antivirus...

L’ingegneria sociale

- Attacchi più mirati
- Spear Phishing: mail indirizzata ad una persona o un’azienda specifica da una fonte apparentemente attendibile che però conduce ad un sito web fittizio contenente malware
- Whaling Phishing: attacco phishing rivolto ai dirigenti condotto con avanzate tecniche di ingegneria sociale
- Vishing: L’attacante impersona al telefono un soggetto noto alla vittima

Un esempio



Mettendo il mouse sopra il link della seconda mail, senza cliccare, viene visualizzato nell'angolo in basso un URL che è diverso da quello mostrato: è un modo per identificare le mail di phishing

anci Piemonte

IFEL Fondazione ANCI

Un esempio

Estratto dal libro “L’arte dell’inganno” di Kevin D. Mitnick

Feltrinelli Editore

Un esempio

Il caso Rosemary 1/2

"Ciao, Rosemary. Sono Bill Jorday , della sicurezza informazioni." "Sì?" "Qualcuno del tuo ufficio ti ha mai spiegato le procedure di sicurezza?" "Non mi pare." "Bene, vediamo. Tanto per cominciare non permettiamo a nessuno di installare programmi arrivati da fuori. Questo perché non vogliamo responsabilità per programmi privi di licenza, e anche per evitare problemi di virus." "Certo." "Sai della
politica per le e mail?" "No." "Qual è il tuo indirizzo?" "Rosemary@ttrzine.net." "L'username è Rosemary?" "R Morgan." "Bene. Vorremmo far capire a tutti i nuovi dipendenti che può essere pericoloso aprire un allegato che non aspettano. Arrivano un sacco di virus con le e mai di gente che non conosci. Perciò se arriva una e mail non richiesta devi sempre controllare per essere sicura che la
persona indicata come mittente ti abbia davvero inviato quel messaggio. Capito?"

Un esempio

Il caso Rosemary 2/2

"Sì, ne ho sentito parlare." "Bene, e siamo soliti cambiare la password ogni tre mesi. Tu quando l'hai cambiata?" "Sono qui da appena tre settimane e sto ancora usando la prima." "Va bene, puoi aspettare che scadano i novanta giorni. Però dobbiamo essere sicuri che il personale non usi password
facili da indovinare. Tu ne hai una di lettere e numeri?" "No." "Dobbiamo provvedere. Quale usi?" "Annette, il nome di mia figlia." "Non è abbastanza sicura. Non usare mai password con i nomi dei familiari. Vediamo ... potresti fare come me. Va bene usare l'attuale come prima parte della password, però ogni volta che la cambi aggiungi il numero del mese corrente." "Quindi, se lo faccio adesso che è marzo, sarà 3 o 03." "Vedi tu. Come credi meglio." "Facciamo Annette3 ." "Bene. Vuoi che ti spieghi come si fa a cambiare?" "No, lo so." "Bene. C'è un'ultima cosa. Tu hai un antivirus nel computer ed è importante tenerlo aggiornato. Non devi mai disattivare www.nomeantivirus.com l'aggiornamento automatico anche se ogni tanto il computer rallenta. Va bene?" "Certo." "Perfetto. E hai il nostro numero per chiamarci se ci sono problemi con il computer?" Non ce l'ha. Lui le dà il numero, lei lo trascrive con attenzione e poi torna all'opera,
contenta di essere seguita tanto premurosamente

Un esempio

BEC: Business Email Compromise

Non contengono link o malware quindi passano indenni i filtri

Per funzionare devono essere altamente personalizzate

Caso reale: nel 2017 un dirigente di Confindustria ha fatto un bonifico di 500.000 € verso un conto estero, perché credeva di aver ricevuto una mail dalla direttrice generale, in quanto gli era arrivata dal suo indirizzo

Anche la PEC è un possibile vettore di malware: non è più sicura della mail semplice. Possono contenere link e allegati pericolosi, spesso racchiusi in file zip, per mascherare meglio il codice malevolo

> È caccia ai ladri. È caccia al tesoro rubato a Poste. È caccia alla banda che ha messo a segno un colpo da 5 milioni di euro. È bastata un'email con una lettera diversa. Una "l" al posto di una "i" per indurre in errore una funzionaria: "@mlcrosoft" in sostituzione all'originale "@microsoft".

anci Piemonte

IFEL Fondazione ANCI

WiFI

Collegarsi ad una rete pubblica può essere molto pericoloso

Un hacker potrebbe avere accesso ai dati degli utenti ed installare un malware, magari creando un hotspot dall'apparenza legittima

Se proprio devi connetterti, utilizza una VPN e collegati solo a siti https, possibilmente evitando banche o siti contenenti informazioni sensibili

Nella propria rete, usare solo i protocolli WPA2 o WPA3

Consapevolezza (Awareness)

Una delle tecniche più usate è la paura: una finta bolletta esagerata mette in moto istinti difficilmente controllabili

VAK (Vision, Auditory, Kinesthetik), per farti cliccare seguendo l'istinto senza riflettere

Autodifesa: Farsi domande

Perché dovrei ricevere un rimborso per qualcosa che non ho fatto?
Perché dovrebbero offrirmi un servizio gratuito?
Abbiamo mai avuto a che fare con questa azienda?

Formazione IFEL
per i Comuni

Adeguamento dell'infrastruttura digitale

anci Piemonte

DOMANDA 4

Penso che nei prossimi 2 anni la cybersecurity avrà un impatto significativo sul mio Ente?

Votate

Sicurezza fin dall'acquisto

L'AGID ha pubblicato delle linee guida per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici delle pubbliche amministrazioni, la rispondenza di questi ad adeguati livelli di sicurezza.

https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/05/20/sicurezza-procurement-ict-online-linee-guida

Sicurezza nel sistema: le misure minime di sicurezza ICT

L'AGID ha pubblicato le misure minime di sicurezza ICT per le pubbliche amministrazioni

Sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Piano strategico dell'ACN

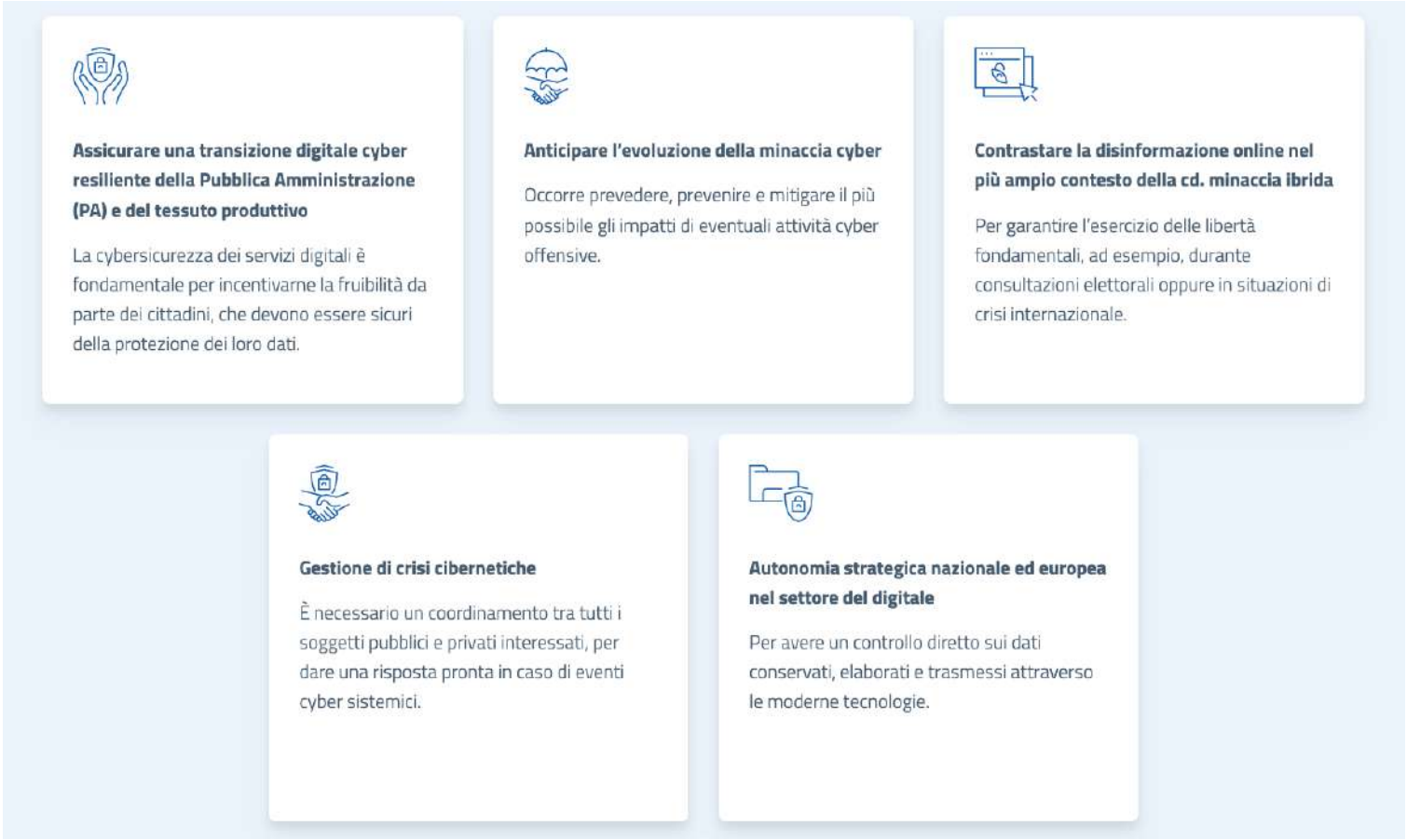
L'Agenzia per la Cybersicurezza Nazionale (ACN) ha pubblicato la Strategia Nazionale di Cybersicurezza, che intende pianificare, coordinare ed attuare misure tese a rendere il Paese più sicuro e resiliente

La strategia prevede il raggiungimento di 82 misure entro il 2026.

L'ACN si occuperà anche di controllare che gli obiettivi vengano raggiunti

https://www.acn.gov.it/strategia-nazionale-cybersicurezza

Piano strategico dell'ACN: le sfide da affrontare



Assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo

La cybersicurezza dei servizi digitali è fondamentale per incentivarne la fruibilità da parte dei cittadini, che devono essere sicuri della protezione dei loro dati.

Anticipare l'evoluzione della minaccia cyber

Occorre prevedere, prevenire e mitigare il più possibile gli impatti di eventuali attività cyber offensive.

Contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida

Per garantire l'esercizio delle libertà fondamentali, ad esempio, durante consultazioni elettorali oppure in situazioni di crisi internazionale.

Gestione di crisi cibernetiche

È necessario un coordinamento tra tutti i soggetti pubblici e privati interessati, per dare una risposta pronta in caso di eventi cyber sistemici.

Autonomia strategica nazionale ed europea nel settore del digitale

Per avere un controllo diretto sui dati conservati, elaborati e trasmessi attraverso le moderne tecnologie.

Piano strategico dell'ACN: gli obiettivi da perseguire

Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

anci Piemonte

IFEL Fondazione ANCI

Promemoria

- Framework Nazionale per la Cybersecurity
- Controlli Essenziali di Cybersecurity
- Rapporto Clusit sulla sicurezza ICT in Italia
- Linee guida per la sicurezza nel procurement ICT
- Misure Minime di sicurezza AGID
- La Strategia Nazionale di Cybersicurezza di ACN

anci Piemonte

IFEL Fondazione ANCI

Conclusioni

- La cybersecurity è ormai di fatto indispensabile, anche per gli Enti più piccoli
- Occorre preparazione tecnica, amministrativa, manageriale
- L'Italia si muove compatta: attuiamo nei prossimi anni la strategia nazionale di cybersicurezza di ACN
- Sentiamoci squadra: siamo piccoli ma tanti e, se remiamo tutti dalla stessa parte, andremo lontano!

anci Piemonte

IFEL Fondazione ANCI

Q & A

Massimo Massimino

Linkedin: https://www.linkedin.com/in/massimo-massimino-343a763a/
Twitter: @mass_massimino

I materiali didattici saranno disponibili su
www.fondazioneifel.it/formazione