CITTA' DI TORINO

CYBERSECURITY

Massimo Massimino

Dirigente del Servizio Infrastrutture e Cybersecurity
Referente per la Cybersicurezza

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

CITTA' DI TORINO

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

CITTA' DI TORINO

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

- Oggi è molto difficile non lasciare tracce che permettono una rapida identificazione

- E' importante un utilizzo responsabile

CITTA' DI TORINO

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

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.

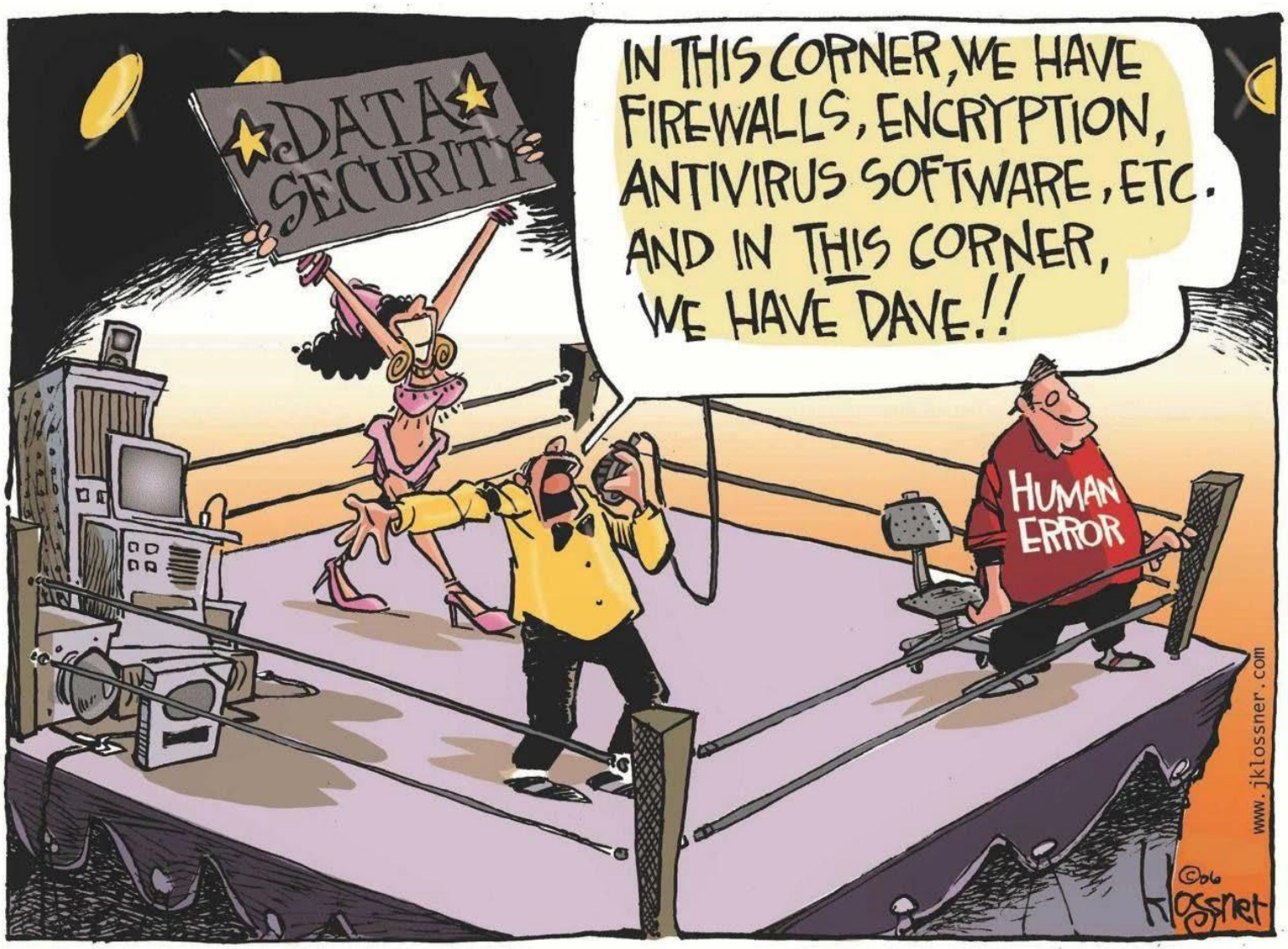
CITTA' DI TORINO

Analisi del rischio

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

CITTA' DI TORINO



CITTA' DI TORINO

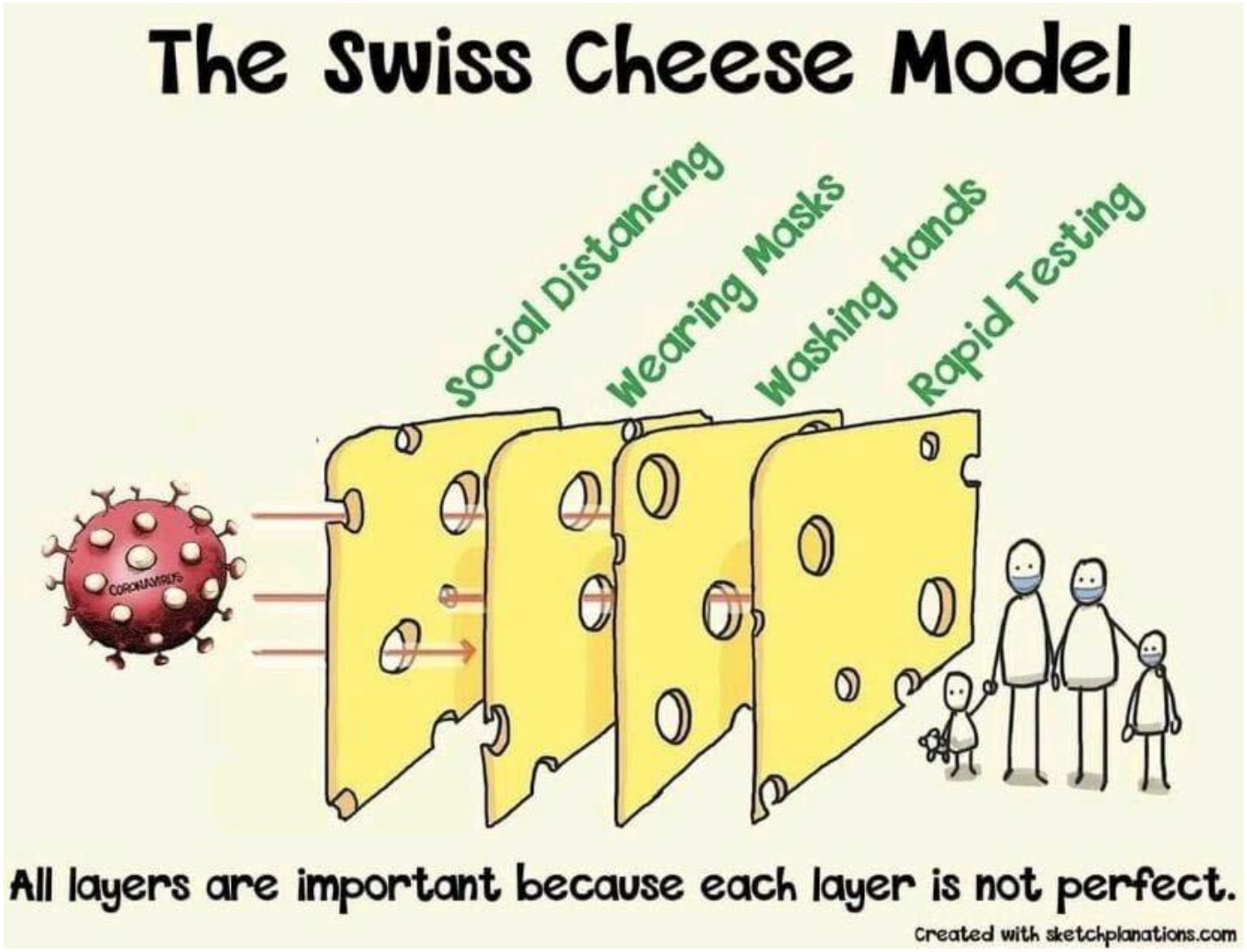
Gestire il rischio

Il Risk Management si compone di 4 fasi

- **Identificazione**: si cerca di identificare le possibili fonti di rischio e individuare i pericoli
- **Valutazione quantitativa e qualitativa**: determinare 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

CITTA' DI TORINO



CITTA' DI TORINO

Il comportamento

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...

CITTA' DI TORINO

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’attaccante impersona al telefono un soggetto noto alla vittima

CITTA' DI TORINO

Un esempio

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

Feltrinelli Editore

CITTA' DI TORINO

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

CITTA' DI TORINO

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".

CITTA' DI TORINO

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

CITTA' DI TORINO

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?

In caso di dubbio scrivere a cybersecurity@comune.torino.it

CITTA' DI TORINO

Le norme sulla cybersicurezza

DL 105 del 21 settembre 2019

Crea il perimetro di sicurezza nazionale cibernetica

Legge 90 del 28 giugno 2024

- Rafforzamento della cybersicurezza nazionale
- Torino entra nel perimetro di sicurezza nazionale
- Referente per la cybersicurezza

D.lgs 138 del 4 settembre 2024

- Recepimento della direttiva europea UE 2022/2555 NIS 2 per livello comune elevato di cybersicurezza nell'UE
- Torino è un soggetto importante e deve avere un "punto di contatto"
- Attivare le misure minime di cybersicurezza entro ottobre 2026

CITTA' DI TORINO

Le misure minime

- Segnalazione degli incidenti cyber entro 24 ore
- Strategia di gestione del rischio
- Ruoli e responsabilità
- Formazione e consapevolezza
- gestione degli asset e degli accessi (MFA)
- gestione delle vulnerabilità
- gestione del software
- sicurezza dei dati
- protezione delle reti
- Cloud certificato
- Sicurezza della catena dei fornitori
- gestione della crisi e piano di risposta agli incidenti

CITTA' DI TORINO

Corso di formazione sulla cybersecurity

La formazione è uno dei pilastri della cybersecurity

Corso triennale sull'awareness del rischio informatico, obbligatorio per tutti i dipendenti

Campagne di phishing mirate

Competizione tra le divisioni

Il nostro corso

CITTA' DI TORINO

Conclusioni

- La cybersecurity è ormai di fatto indispensabile, nel lavoro e nella vita privata
- Occorre preparazione tecnica, amministrativa, manageriale, soprattutto in caso di crisi non si può improvvisare!!
- Attuiamo nei prossimi anni la strategia nazionale di cybersicurezza e le prescrizioni della direttiva NIS 2
- Sentiamoci squadra!

CITTA' DI TORINO

Grazie per l’attenzione

Benvenute e benvenuti a bordo!

CITTA' DI TORINO