Cofinanziato dall'Unione europea

EYESonCS

EyesOnCS
Compendio di casi di sicurezza informatica

Italiano
Ottobre 2023

Dati del progetto

Acronimo: EyesOnCS

Titolo: Miglioramento della sicurezza informatica – Sviluppo di corsi di formazione utilizzando il modello "Escape Room"

Progetto n.: 2021-1-DE02-KA220-VET-000033003

Durata: 01. Gennaio 2022 - 31. Dicembre 2023 (24 mesi)

Programma: Erasmus+, Azione chiave 2, Partenariati di cooperazione nel campo dell'istruzione e formazione professionale

Coordinatore: Fachhochschule des Mittelstands (FHM)

Edizione: Ottobre 2023

Organizzazioni partner del progetto

Staatlich anerkannte, private Fachhochschule des Mittelstands (FHM)

virtualcampus

AKADEMIE ASW

fb finance & banking Associazione per lo sviluppo organizzativo e delle risorse umane

Restate sintonizzati!

Per saperne di più sul progetto seguiteci qui:

www.eyesoncs.eu

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

Indice

1 Introduzione 4
2 Strategie nazionali ed europee 6
3 Le sfide delle PMI 9
4 Ruolo dell'istruzione e della formazione - Concetti rilevanti per la formazione sulla cybersecurity 12
4.1 Apprendimento basato sul gioco 13
4.2 Escape Rooms Educative (ERE) 14
5 Casi di sicurezza informatica 16
5.1 🇮🇹 Casi di sicurezza informatica in Italia 17
5.2 🇩🇪 Casi di sicurezza informatica dalla Germania 30
5.3 🇵🇹 Sicurezza informatica Casi dal Portogallo 55
6 Conclusioni 63
7 Bibliografia 64

Immagini

Figura 1: Posta elettronica. 18
Figura 2: Accesso a Microsoft. 18
Figura 3: Notifica di errore da parte del server di posta elettronica ricevente. 31
Figura 4: Intestazione della mail di spam. 31
Figura 5: Nota di sicurezza. 37
Figura 6: L'allegato pericoloso. 39

1. Introduzione

Non c'è giorno che non avvenga un crimine informatico. La situazione della criminalità informatica nel mondo è aumentata in modo significativo negli ultimi anni. Una delle ragioni è la continua digitalizzazione in quasi tutte le sfere del lavoro e della vita. Mentre in passato i crimini e gli attacchi erano caratterizzati da una rapina in banca o da un altro attacco fisico, oggi sono caratterizzati da un aggressore seduto su una spiaggia, con un computer portatile, che accede illegalmente al sistema di distribuzione di una banca per estorcere un riscatto. L'associazione di settore Bitcom conta oltre 220 miliardi di euro di danni all'anno. Per le piccole e medie imprese un attacco e la sottrazione di segreti commerciali possono significare la rovina economica (Streim, A., Mann, S. (2021)). La pandemia Covid19 ha anche reso possibili nuovi formati di lavoro in un breve periodo di tempo. Le misure di protezione corrispondenti non sono state stabilite o adattate in parallelo. Questo apre la strada ad attacchi alla sicurezza e a vulnerabilità per gli invasori e i trasgressori. Per questo motivo, è estremamente importante informare i dipendenti sugli effetti e le conseguenze di un attacco informatico e sensibilizzarli di conseguenza.

Questo compendio è stato sviluppato nel contesto del progetto Erasmus+ "EyesOnCS". Il team del progetto persegue diversi obiettivi con lo sviluppo di questa pubblicazione:

In primo luogo, una panoramica introdurrà le strategie per l'applicazione della cybersecurity (CS), soprattutto nelle PMI. In seguito, vengono discusse le sfide particolari che le PMI devono affrontare nell'implementazione della cybersecurity. Successivamente, il compendio si concentra brevemente sull'importanza dell'istruzione e della formazione per prevenire gli attacchi di CS. Segue una raccolta completa di casi di cybersecurity che si sono verificati nella pratica. Questi casi sono stati raccolti dal team internazionale del progetto presso aziende e altre istituzioni e sono documentati in dettaglio ai fini del presente compendio.

I gruppi target di questo compendio sono principalmente le aziende e le istituzioni educative che possono utilizzare i casi di CS raccolti a scopo formativo.

Dopo un'introduzione al tema generale della sicurezza, il secondo capitolo tratta delle principali strategie di CS nazionali ed europee. In questo contesto, viene spiegato ed evidenziato il ruolo dell'ENISA (Agenzia dell'Unione Europea per la Cybersecurity). A questo proposito, la Relazione annuale consolidata sulle attività dell'ENISA afferma: "Nel 2021, l'ENISA ha dovuto affrontare le sfide portate dalla pandemia, che ha influito sulle attività di sviluppo delle capacità a più livelli. Da un lato, per ovvie ragioni, è stato necessario convertire diversi corsi ed esercitazioni per l'erogazione online. Questo cambiamento ha posto alcune sfide fin dalla conversione"[1].

1 ENISA: Consolidated Annual Activity Report 2021, Attiki, 2022

Inoltre, in questo capitolo il compendio si concentra sulla legge europea sulla cybersecurity, che introduce un quadro di certificazione della cybersecurity a livello europeo per i prodotti, i servizi e i processi delle tecnologie dell'informazione e della comunicazione (TIC). Le aziende che operano nell'UE beneficeranno del fatto che dovranno certificare i loro prodotti, processi e servizi ICT una sola volta e vedranno i loro certificati riconosciuti in tutta l'Unione Europea.[2]

Inoltre, in questo secondo capitolo, il compendio cerca di registrare e presentare le varie strategie di sicurezza nazionali. Per ragioni pratiche, l'elenco non è esaustivo. Vengono illustrate, tra le altre, le seguenti:

- l'associazione tedesca "Deutschland sicher im Netz e.V. (DsiN)[3]"
- il CERT-Bund[4], un Computer Emergency Response Team per le autorità federali
- la Strategia Nazionale Italiana di Cybersecurity per il 2022/26 e
- il Centro nazionale portoghese per la sicurezza informatica (CNCS).

Il terzo capitolo riassume le sfide per le PMI in materia di cybersecurity. A tal fine, gli autori utilizzano il triplice approccio dell'ENISA, comprese le raccomandazioni per le PMI.[5] A questo proposito, il compendio copre le seguenti aree:

- Area Persone
- Area Processi
- Area Tecnica.

Questo progetto mira a implementare particolari raccomandazioni per le PMI a livello educativo. Le raccomandazioni ENISA per le PMI6 si concentrano su tre aree diverse. Questo compendio elenca una serie di domande guida per i controlli di CS e anche per la valutazione dei casi pratici di CS raccolti (vedi capitolo 5).

Inoltre, il progetto mira a sviluppare speciali metodi di formazione virtuale sulla CS e a implementarli sulla base di cosiddetti scenari. Pertanto, nel capitolo 4 del compendio vengono descritti e valutati concetti rilevanti per la formazione in CS. Questi includono l'apprendimento basato sui giochi e le stanze di fuga educative (EER).

Una parte particolarmente importante ed estesa del compendio consiste nella descrizione e nella valutazione sintetica di casi pratici di CS che i partner del progetto hanno ricercato, compilato e valutato nei rispettivi Paesi di origine, Italia, Germania e Portogallo. Il capitolo 5 descrive 26 di questi casi pratici in una forma uniformemente strutturata e comparativa.

---

2 EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 32019R0881 - EN - EUR-Lex.

3 Deutschland sicher im Netz, https://www.sicher-im-netz.de.

4 Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html.

5 ibid.

2 Strategie nazionali ed europee

A livello europeo, le strategie di prevenzione della criminalità e di sicurezza informatica sono ancora in fase di sviluppo. Esistono già alcuni approcci validi, ma restano altrettante sfide da affrontare. Attualmente sono poche le agenzie governative che si occupano di questo tema, che sta particolarmente a cuore alle PMI.

Una di queste è l'ENISA (European Union Agency for Cybersecurity)[6], la quale si preoccupa che in tutta Europa venga raggiunto un elevato livello di sicurezza informatica. L'ENISA sostiene attivamente la politica dell'Unione Europea per aumentare la sicurezza informatica e l'affidabilità dei prodotti e dei servizi delle tecnologie dell'informazione e della comunicazione attraverso la certificazione della sicurezza informatica. Inoltre, l'Agenzia contribuisce a rafforzare le difese dell'infrastruttura dell'Unione e, in ultima analisi, a garantire un ambiente digitale sicuro per la società e i cittadini europei.

La passata pandemia di Covid19 ha fatto si che l'attività “in rete” (l’utilizzo di internet) dei cittadini europei aumentasse, sia in ambito professionale che privato. Purtroppo aprendo ulteriori varchi per attacchi puntuali e coordinati. Gli aggressori della rete sono riusciti ad insinuarsi con maggiore facilità a causa della mancanza di know-how e solide strutture di difesa. Data la delicata e compromettente situazione, l’ENISA ha ancora di più ed in modo più significativo intensificato le attività di lotta al crimine. A questo proposito, il Rapporto Annuale delle Attività dell'ENISA afferma: "Nel 2021, l'ENISA ha dovuto affrontare le sfide lanciate dalla pandemia, che hanno influito sulle attività di sviluppo a più livelli. Ad esempio, per ovvie ragioni, è stato necessario convertire diversi corsi ed esercitazioni per l'erogazione online. Questo cambiamento ha posto non poche difficoltà.[7]

Nel 2019 l'Agenzia dell'UE per la cybersicurezza è diventata più forte grazie alla legge sulla cybersicurezza dell'UE.[8] La legge conferisce un mandato permanente all'agenzia e le assegna maggiori risorse e nuovi compiti. Ora l'ENISA avrà un ruolo chiave nella creazione e nel mantenimento del Quadro Europeo di Certificazione della cybersicurezza, preparando il terreno tecnico per gli schemi di certificazione specifici, supervisionando attraverso un sito web dedicato il livello di informazione del pubblico sui suddetti schemi di certificazione e sui certificati rilasciati. l'ENISA è incaricata di aumentare la cooperazione operativa a livello Europeo, aiutando gli Stati Membri che richiedono assistenza a gestire i loro incidenti di cybersicurezza e sostenendo il coordinamento dell'UE in caso di crisi e attacchi informatici transfrontalieri su larga scala.

---

6 https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity
7 ENISA: Consolidated Annual Activity Report 2021, Attiki, 2022
8 EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 320 19R0881 - EN - EUR-Lex.

Inoltre, l'EU Cybersecurity Act introduce un Quadro di Certificazione della cybersecurity a livello Europeo per i prodotti, i servizi e i processi delle tecnologie dell'informazione e della comunicazione (TIC). Le aziende che operano nell'UE beneficeranno del fatto che dovranno certificare i loro prodotti, processi e servizi ICT una sola volta e questi certificati saranno riconosciuti a livello Europeo. Il quadro di certificazione della cybersecurity dell'UE per i prodotti ICT consente la creazione di schemi di certificazione a livello europeo basati sul rischio, personalizzati fornendo altresì un insieme completo di regole, requisiti tecnici, standard e procedure. Il quadro attesterà che i prodotti e i servizi TIC che sono stati certificati secondo schema sono conformi ai requisiti.[9]

A livello nazionale, in **Germania**, l'associazione "Deutschland sicher im Netz e.V. (DsiN)"[10] supporta i consumatori e le piccole imprese nel rapportarsi in modo sicuro e fiducioso con il mondo digitale, oltre a offrire opportunità di apprendimento per le persone in ambito privato e professionale.

Un altro supporto molto valido e utile per le PMI è il CERT-Bund[11], il Computer Emergency Response Team per le autorità federali, che è il punto di contatto centrale per le misure preventive e reattive in caso di incidenti legati alla sicurezza dei sistemi informatici. Oltre al supporto per le autorità federali, il CERT cittadino fornisce informazioni gratuite sugli attuali attacchi di malware e sulle vulnerabilità di sicurezza delle applicazioni informatiche.

Nel Maggio 2022, **l'Italia** ha annunciato la sua Strategia Nazionale di Cybersecurity per il periodo 2022-2026, un documento fondamentale per affrontare le minacce informatiche e aumentare la resilienza del Paese. La strategia, sviluppata dall'Agenzia Nazionale Italiana per la Sicurezza Informatica, comprende 82 obiettivi e mira ad affrontare le seguenti sfide:

- Assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del sistema produttivo.
- Prevedere l'evoluzione delle minacce informatiche per ridurre il loro impatto sulle infrastrutture e sulle organizzazioni nazionali.
- Prevenire la disinformazione online in un contesto più ampio di minaccia ibrida.
- Gestire le crisi informatiche.
- Rafforzare l'autonomia strategica nazionale ed europea del settore digitale.

La strategia italiana per la cybersecurity coniuga sicurezza e sviluppo, nel rispetto dei valori della nostra Carta Costituzionale. Essa tiene conto delle disposizioni della strategia di cybersecurity dell'Unione Europea del dicembre 2020, della Bussola Strategica per la Sicurezza e la Difesa dell'UE del Marzo 2022 e delle recenti linee guida strategiche della NATO. Per realizzare questa nuova visione, l'Italia ha concepito un ecosistema di cybersecurity

9 European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.
10 Deutschland sicher im Netz, https://www.sicher-im-netz.de.
11 Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

basato sulla collaborazione tra settore pubblico e privato. In tale sistema, al contributo attivo delle Istituzioni si affianca quello degli operatori economici – in primis quelli cui è affidata la gestione delle infrastrutture da cui dipende l'erogazione di servizi essenziali da parte dello Stato – del mondo dell'università e della ricerca, nonché della società civile.[12]

In **Portogallo**, il Centro Nazionale per la Sicurezza Informatica (CNCS) è il coordinatore operativo e l'autorità nazionale portoghese specializzata nella sicurezza informatica che collabora con gli enti statali, gli operatori di servizi essenziali e i fornitori di servizi digitali, assicurando che il cyberspazio sia utilizzato come uno spazio di libertà, sicurezza e giustizia, per la protezione di tutti i settori della società.[13] La missione del CNCS è contribuire all'uso libero, affidabile e sicuro del cyberspazio in Portogallo, attraverso il continuo miglioramento della sicurezza informatica nazionale e della cooperazione internazionale, in coordinamento con tutte le autorità competenti, e l'attuazione delle misure e degli strumenti necessari per l'anticipazione, l'individuazione, la reazione e il recupero di situazioni che possono compromettere il funzionamento delle infrastrutture critiche e gli interessi nazionali. Il CERT.PT coordina la risposta agli incidenti che coinvolgono enti statali, operatori di infrastrutture critiche, operatori di servizi essenziali, fornitori di servizi digitali e, in generale, il cyberspazio nazionale in Portogallo.

12 ACN Italy: National Cybersecurity Strategy 2022 – 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, seen 29.7.22
13 Cyber security intelligence: National Cyber Security Centre Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html.

3. Le sfide delle Piccole e Medie Imprese (PMI)

Gli attacchi informatici possono minare l'attività delle Piccole e Medie Imprese (PMI). Le PMI sono spesso aziende a conduzione familiare la cui produzione e le cui strategie commerciali si basano su una lunga tradizione. In pratica, ciò è spesso in netto contrasto con le misure di protezione prevalenti, che di solito sono associate a costi considerevoli e/o non dispongono del know-how corrispondente. Il numero di attacchi informatici alle PMI è aumentato esponenzialmente negli ultimi tre anni. Inoltre, sono sempre più spesso oggetto di spionaggio economico e industriale mirato. I dipendenti dei dipartimenti di sicurezza aziendale hanno conoscenze di base, un adeguato livello di consapevolezza e ricevono una formazione interna a intervalli regolari. In caso di attacco, le responsabilità e le procedure sono definite e provate. Tutte queste strutture non sono generalmente presenti nelle PMI. La maggior parte dei dipendenti non sa come gestire i dati sensibili. Questo non solo mette a rischio la capacità dell'azienda di operare, ma anche, nel peggiore dei casi, molti posti di lavoro. Dopo tutto, anche le PMI fanno parte della catena di approvvigionamento. Un attacco informatico a una PMI può quindi avere un forte impatto sulla catena di fornitura e ripercussioni su un'agenzia governativa o su altre grandi aziende.

Secondo un recente sondaggio[14], oltre l'80% delle PMI europee ha dichiarato che i problemi di cybersecurity avrebbero un grave impatto negativo sulla loro attività entro una settimana dal verificarsi di un attacco, e il 57% ha affermato che molto probabilmente andrebbero in bancarotta o chiuderebbero l'attività. Ciononostante, le PMI non sembrano rendersi conto che la sicurezza informatica non è un problema che riguarda solo le grandi organizzazioni. Le PMI devono quindi essere consapevoli dell'impatto che i problemi di cybersecurity possono avere sulla loro attività. Molte PMI ritengono che i controlli di sicurezza inclusi nei prodotti informatici che acquistano siano sufficienti e che non sia necessario farne degli ulteriori, a meno che non siano imposti da normative o leggi. Il presente compendio intende contribuire a fare maggiore chiarezza a questo proposito. Pertanto, l'ENISA propone un triplice approccio che comprende raccomandazioni per le PMI[15]:

- Area Persone
- Area Processi
- Area Tecnica.

Questo progetto mira a implementare le seguenti raccomandazioni delle PMI a livello educativo. Esse comprendono il mantenimento di software aggiornati, l'applicazione di regole rigorose di controllo degli accessi, l'utilizzo di servizi cloud e altro ancora.
Le raccomandazioni delle PMI dell'ENISA[16] si concentrano su tre aree diverse. All'interno delle aree sono elencati i principali punti di controllo, comprese le domande guida. Questo elenco può essere utilizzato anche come questionario per un autotest.

14 ENISA: Cybersecurity for SMES- Challenges and Recommendations, European Union Agency for Cybersecurity (ENISA), Attiki, 2021
15 ibid.
16 ibid.

Domande guida per l'Area PERSONE

Responsabilità	Un direttore, o un suo equivalente, ha la responsabilità della cybersecurity?
Coinvolgimento dei dipendenti	Tutti i membri del personale hanno dichiarato per iscritto di aver letto, compreso e accettato la politica di sicurezza delle informazioni?
Sensibilizzazione dei dipendenti	Tutti gli utenti dei vostri sistemi informatici ricevono una formazione regolare sulle loro responsabilità in materia di sicurezza, su come identificare e affrontare le varie minacce alla sicurezza? Assicuratevi che il personale sia a conoscenza e possa verificare tutti i punti di contatto e i canali di comunicazione.
Formazione sulla sicurezza informatica	I membri del personale con responsabilità specifiche in materia di sicurezza ricevono una formazione adeguata e regolare a supporto del loro ruolo?
Politiche di sicurezza informatica	Avete una politica di sicurezza documentata, con le relative procedure operative, firmata e pienamente supportata dal senior management?
Gestione di parti terze	L'alta direzione autorizza l'accesso di terzi a informazioni riservate e/o commercialmente sensibili in attesa della compilazione di appositi moduli di riservatezza?

Domanda guida per l'Area PROCESSI

Audits	I sistemi critici, come i firewall e i router, vengono regolarmente testati per individuare eventuali vulnerabilità? I computer vengono controllati per verificare che non siano presenti copie di software illegale?
Pianificazione e risposta agli incidenti	Esiste un piano di gestione degli incidenti di sicurezza?
Password	Tutte le password predefinite su tutti i sistemi vengono ripristinate rispetto a quelle installate dal fornitore? Gli utenti sono costretti a utilizzare password complesse e difficili da indovinare?

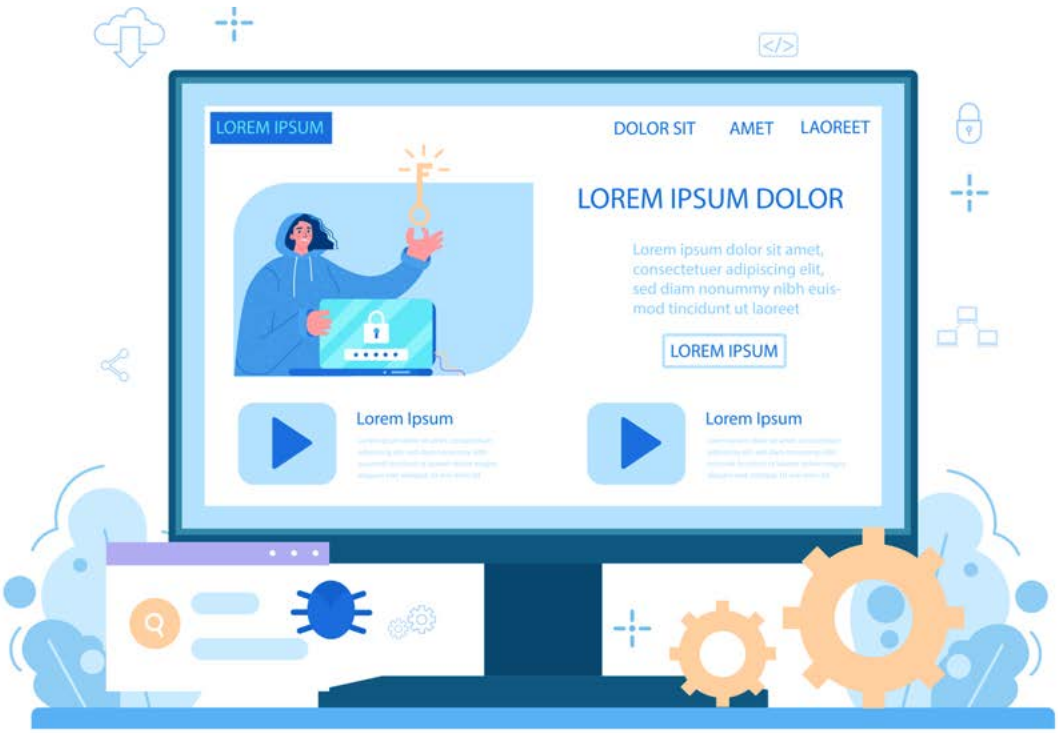
Patch del software	Esiste un meccanismo per garantire che le patch di sicurezza critiche vengano distribuite ai sistemi in modo tempestivo e controllato?
Protezione dei dati	I sistemi e i database che memorizzano i dati personali sono protetti in modo adeguato a garantire la conformità ai requisiti normativi e legali, come il Regolamento generale sulla protezione dei dati dell'UE, la legge sulla sicurezza informatica[17] e la legge sulla protezione dei dati?

Domanda guida per l'AREA TECNICA

Sicurezza di rete	Le connessioni esterne, ad esempio a Internet, sono autorizzate dal senior management, adeguatamente documentate e protette da firewall?
Anti-Virus	Tutti i sistemi informatici sono protetti dal software anti-virus più aggiornato? Gli utenti sono istruiti su come identificare e gestire le e-mail o i file sospetti che possono contenere virus informatici?
Crittografia	Tutti i dispositivi che memorizzano dati sono dotati di crittografia completa del disco? Utilizzate reti private virtuali (VPNS) quando comunicate via Internet su reti pubbliche?
Monitoraggio della sicurezza	I file di log dei dispositivi di sicurezza importanti sono monitorati attivamente per rilevare potenziali violazioni della sicurezza?
Sicurezza fisica	• Le risorse informatiche critiche, come i file server, sono protette in un'area protetta dall'accesso non autorizzato? • Sono state adottate misure per l'home office che garantiscano aree protette paragonabili all'ufficio (porte chiuse quando si lascia il posto di lavoro, nessun accesso alle informazioni da parte di terzi attraverso finestre o altro)?
Backup sicuri	Un buon backup può salvare la vostra azienda da un attacco ransomware. Eseguite regolarmente il backup dei dati e dei sistemi critici in un archivio offline sicuro? Testate regolarmente il ripristino dai vostri backup per verificare la possibilità di ripristinare completamente i vostri dati e sistemi?

17 European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

4. Ruolo dell'Istruzione e Formazione Professionale – Concetti rilevanti per la formazione sulla cybersecurity



Le aziende non sempre riconoscono il fatto che il successo della cybersecurity non dipende solo dalla protezione tecnica, ma anche, in larga misura, dalla sensibilizzazione e dalla fiducia dei dipendenti nell'agire. Sebbene un'azienda su quattro identifichi costantemente la necessità di intervenire sulla sicurezza aziendale e metta a disposizione maggiori risorse, l'attenzione si concentra chiaramente sulla protezione tecnica. Nelle PMI spesso la formazione e la sensibilizzazione dei dipendenti avviene solo in misura limitata. Ciò significa che si presta poca attenzione al fattore di protezione umano, che diventa ancora più importante con il lavoro mobile e l'home office. La sensibilizzazione sui rischi per la sicurezza associati ai luoghi di lavoro flessibili sta diventando sempre più necessaria. Ovviamente, è importante sensibilizzare le aziende sulle nuove opportunità di attacco che possono derivare dal lavoro da remoto.
È quindi consigliabile offrire corsi di formazione specifici. Inoltre, è utile sensibilizzare le aziende con informazioni scritte o attraverso eventi istituzionali.

4.1 Apprendimento basato sul gioco

I videogiochi sono apparsi sul mercato dei consumatori circa 50 anni fa e il loro impatto sociale e culturale è aumentato esponenzialmente fino a diventare un elemento fondamentale (Oblinger 2006). I giochi sono sistemi endogeni, con attività di problem solving strutturate da meccaniche e regole di gioco. L'impegno nei giochi e nel gioco è motivato internamente, nel senso che gli individui vi partecipano volontariamente. I giochi descrivono l'interazione tra il giocatore e gli elementi del gioco che portano a comportamenti e producono risultati diversi. In larga misura, i giochi permettono al giocatore di scegliere, il che favorisce la sua immersione, un fenomeno sperimentato da un individuo quando si trova in uno stato di profondo coinvolgimento mentale (Agrawal et al, 2020). Ma i giochi contribuiscono anche alla socializzazione e aiutano i giocatori a creare connessioni tra la causa e l'effetto delle loro decisioni, il che può contribuire al pensiero critico e logico. Inoltre, migliorano diverse abilità cognitive, intrapersonali e interpersonali come la percettività, l'attenzione, la memoria, l'analisi e la sintesi visiva e uditiva, il confronto, la classificazione e la generalizzazione.

Se inizialmente si pensava a semplici oggetti di intrattenimento, la progettazione e/o l'utilizzo dei videogiochi per altri scopi è stata vista come un passo logico per sfruttare la motivazione e il coinvolgimento degli utenti. Per questo motivo, i videogiochi sono ora utilizzati nel settore dell'istruzione e della formazione professionale, della pubblicità, negli studi di ricerca, per le campagne di salute pubblica, ecc. Questi giochi, chiamati Serious Games, sono genericamente definiti come "[giochi] che non hanno come scopo primario l'intrattenimento, il piacere o il divertimento" (Michael e Chen 2006, p. 21) o come "... una gara mentale, giocata con un computer secondo regole specifiche, che utilizza il divertimento per promuovere obiettivi di formazione governativa o aziendale, istruzione, assistenza sanitaria, consapevolezza sociale, politiche pubbliche, gestione delle crisi e comunicazione strategica" (Zyda 2005, p. 26). I Serious Game esplorano la motivazione intrinseca e l'immersione dei giocatori attraverso l'uso di meccaniche e dinamiche di gioco adeguate a sviluppare abilità e competenze specifiche, per trasmettere all'utente un'informazione (o un messaggio) desiderata o per rafforzare le conoscenze o la consapevolezza acquisite mentre quest'ultimo è immerso in un ambiente ludico.

L'istruzione è l'area con il maggior numero di esempi (di successo) di utilizzo dei Serious Games, generando così il termine "game-based learning", che si riferisce a giochi progettati con obiettivi di apprendimento specifici. Gli utenti possono "imparare facendo" e "imparare sbagliando" in un ambiente controllato che supporta lo sviluppo di conoscenze, abilità e competenze e può persino migliorare il lavoro di squadra, le abilità sociali, la leadership e la collaborazione (Juzeleniene et al. 2014).

L'apprendimento basato sul gioco mira a estrarre le componenti che rendono attraente il gioco e a combinarle con le informazioni e le conoscenze desiderate da trasmettere all'utente,

creando una fonte interattiva per l'apprendimento che, a sua volta, motiva ogni utente ad ampliare le proprie conoscenze e ad approfondire lo studio in un approccio stimolante, coinvolgente e immediato (Prensky, 2003). I seguenti vantaggi sono stati correlati all'uso dei giochi educativi (Abt, 1987):

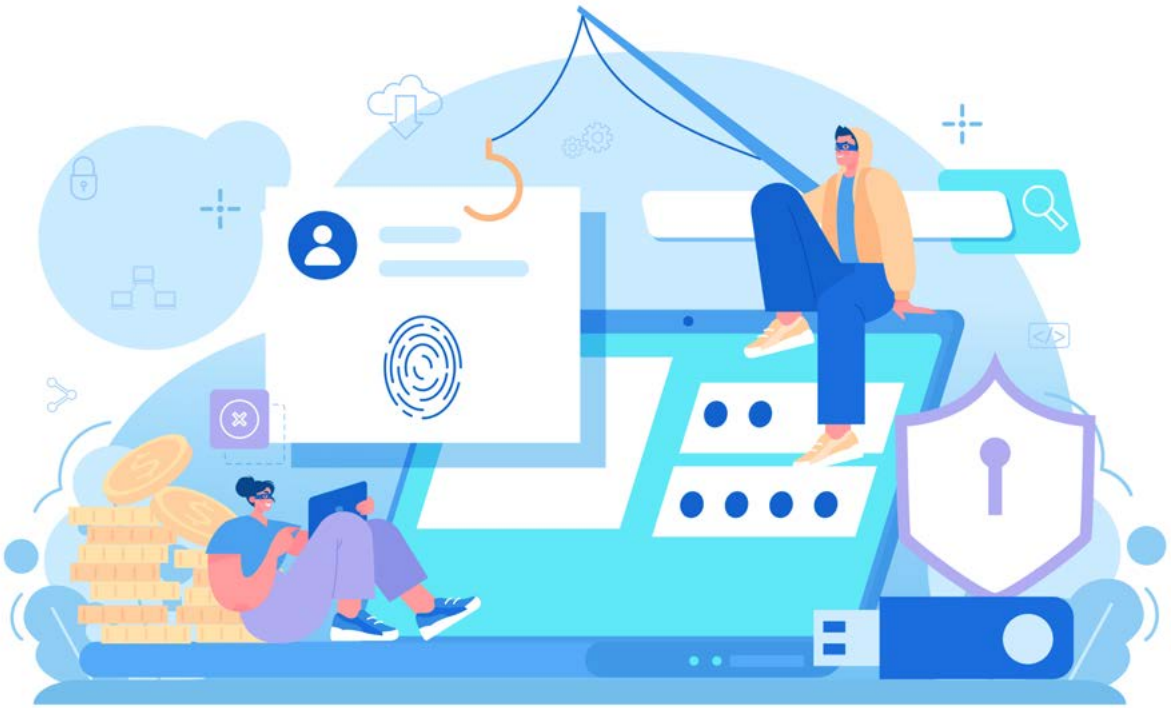
- I giochi introducono gli utenti ai problemi e alla loro risoluzione. Possono essere utilizzati per motivare gli studenti a impegnarsi nei processi educativi, incoraggiandoli a creare e collaborare.
- I giochi hanno obiettivi chiari. Se progettati con cura possono essere collegati a quelli educativi, contribuendo al raggiungimento dei risultati di apprendimento scolastico.
- Attraverso l'elemento visivo, i giochi contribuiscono a una migliore comprensione dei concetti astratti.
- I giocatori si immergono in ruoli realistici, progettano strategie e prendono decisioni. Ciò contribuisce allo sviluppo del pensiero critico e analitico e della capacità di risolvere i problemi.
- I giochi forniscono un feedback in tempo reale. Questo facilita la comprensione delle conseguenze delle loro scelte, scoprendo i legami tra causa ed effetto, contribuendo a creare la struttura della conoscenza.
- I giochi possono aiutare gli studenti fare valutazioni in un ambiente sicuro. Possono anche essere utilizzati per la valutazione autentica, simulando contesti reali.
- I giochi sono utili ed efficaci per la formazione (iniziale) che riguarda processi e pratiche pericolose o quando utilizzare spazi fisici diventa costoso.

4.2 Escape Rooms Educative (ERE)

Una "Escape Room" è un gioco in cui una squadra di giocatori scopre indizi, risolve enigmi e svolge compiti in una o più stanze per raggiungere un obiettivo in un periodo di tempo limitato. I giochi sono ambientati in una varietà di luoghi fittizi, come celle di prigione, laboratori e persino stazioni spaziali, a seconda del tema del gioco. Anche gli obiettivi dei giocatori e le sfide che incontrano sono in linea con il tema.
"Lo sviluppo delle Escape Room risale al 2007 in Giappone, dove sono state impiegate per scopi commerciali. Sono diventate ancora più popolari seguito della loro introduzione negli Stati Uniti nel 2013 (Nicholson, 2015)." (Martina, Richard & Göksen, Sultan, 2020)
Il gioco inizia normalmente con una breve introduzione delle regole, trasmessa in forma di video, audio o da un Gamemaster in carne e ossa. I giocatori entrano quindi in una stanza o in un'area dove viene avviato un timer che limita il tempo a disposizione per completare il gioco, che in genere va dai 45 ai 60 minuti. I giocatori esplorano, trovano indizi e risolvono enigmi che permettono loro di avanzare nel gioco. Queste sfide sono generalmente più mentali che fisiche, ma per i diversi tipi di enigmi sono richieste conoscenze e abilità diverse. Se i giocatori si bloccano, possono chiedere suggerimenti, forniti in forma scritta, video o audio, oppure da un Gamemaster in carne e ossa. I giocatori perdono la partita se non riescono a completare

tutti gli enigmi entro il tempo stabilito. La vittoria consiste o nel portare a termine la missione entro il tempo limite o nell'eliminare la minaccia o l'antagonista della storia, mentre i la sconfitta è di solito rappresentata da scenari nei quali i giocatori vengono "uccisi" o portati via da un antagonista della stanza una volta che il tempo a disposizione è scaduto. Oltre al fattore divertimento, le Escape Room possono essere utilizzate anche per incoraggiare la collaborazione, il lavoro di squadra e il team building.
Le Escape Room virtuali sono la controparte digitale dell'Escape Room che si svolge in un ambiente fisico. La squadra comunica e collabora attraverso una piattaforma online, utilizzando un'applicazione software che può essere gestita da un giocatore e condivisa con gli altri. Come nelle Escape Room fisiche, le squadre risolvono gli enigmi in un tempo prestabilito. Le Escape Room digitali più complesse possono utilizzare la realtà virtuale per aumentare il senso di immersione dei giocatori.
Da diversi anni, anche il settore accademico ha cominciato ad utilizzare l'Escape Room virtuale. Da tempo esistono diversi studi scientifici sull'efficacia e sull'uso delle ERE in tutto il mondo. In Europa, le ricerche sull'argomento non sono ancora molto numerose, ma stanno crescendo notevolmente (Tercanli, H. et al. 2021). I modelli di Escape Room sono utilizzati in diversi ambiti tematici. Il progetto EyesOnCS intende adottare l'approccio dell'Escape Room virtuale quale strumento per la formazione delle PMI in materia di cybersicurezza. Il 22% delle ERE utilizzate finora riguarda il campo dell'informatica e quindi fa già parte dei primi 3 studi per i quali sono state utilizzate le ERE (Tercanli, H. et al. 2021).
Le Escape Room Educative sono utilizzate per diverse fasi del processo di apprendimento. Mentre alcune ERE non richiedono alcuna conoscenza preliminare e permettono di apprendere le nozioni di base, altre la richiedono e permettono di approfondire le conoscenze attraverso il loro approccio didattico (Guckian et al. 2020; Mac Gregor, 2018; Tercanli, H. et al. 2022).
Nel complesso, l'utilizzo dell'Escape Room promuove le competenze trasversali, accresce la motivazione e permette di sviluppare soft skills quali problem-solving, il team building, il pensiero critico, creando allo stesso tempo consapevolezza su un determinato argomento. Si tratta quindi di un metodo di apprendimento estremamente efficace che aumenta significativamente le conoscenze di circa il 53%. Il consolidamento delle conoscenze gioca un ruolo importante e viene garantito (Tercanli, H. et al. 2021).
L'approccio Escape Room Model può essere utilizzato anche nelle aziende. EyesOnCS e la conseguente Escape Room sulla sicurezza informatica hanno lo scopo di sensibilizzare e formare i dipendenti (non tecnici) sulla conoscenza dell'argomento. In questo caso si parte già dalle basi e si dà ai giocatori un senso di sicurezza attraverso un apprendimento ludico. Anche in questo caso, come nell'HEI, la curva di apprendimento ripida avrà effetto e verrà data motivazione per un argomento che ad alcuni sembra ancora estraneo.

5 Casi di sicurezza informatica



La prospettiva della cybersecurity, soprattutto per le PMI e le aziende, è preoccupante. Il livello di protezione delle aziende non è adeguato alla costante crescita dell'innovazione digitale. Molte persone sono anche poco attente nell'uso dei propri dispositivi digitali nel privato divulgando inconsapevolmente informazioni sensibili e personali su Internet. È importante mostrare i pericoli e le conseguenze di questo comportamento e spiegare come gestire le informazioni professionali in modo appropriato. Poiché le piccole e medie imprese garantiscono la stabilità economica di molti Paesi europei, è necessario sensibilizzare i dipendenti per rendere l'Europa più resiliente.
Questo compendio fornisce ai lettori esperienze concrete su casi di cybersecurity raccolti dai diversi partners nei loro paesi di provenienza: Italia, Germania e Portogallo. Questi casi sono descritti in dettaglio nel capitolo seguente.

5.1 Casi di sicurezza informatica in Italia

Caso 1 – L'importanza dei firewall nella sicurezza informatica

Titolo	L'importanza dei firewall nella sicurezza informatica
Fonte	Post e Italiane PST - National Postal service company (Italy)
Periodo di riferimento	Agosto 2021
Tag	Azienda, Furto d'identità, Attacco via e-mail, Phishing
Stato	Risolto entro la fine di agosto 2021 con la modifica delle credenziali di accesso
Applicabilità Escape Room	Altamente trasferibile: Si tratta di un caso comune che può essere facilmente compreso.

Eyes on phishing:
Gli attacchi di phishing prevedono l'invio in massa di e-mail fraudolente a utenti ignari, camuffate come se provenissero da una fonte affidabile. Le e-mail fraudolente hanno spesso l'apparenza di essere legittime, ma collegano il destinatario a un file o a uno script dannoso progettato per consentire agli aggressori di accedere al dispositivo per controllarlo o raccogliere informazioni, installare script/file pericolosi o estrarre dati come informazioni sull'utente, informazioni finanziarie e altro ancora. Gli attacchi di phishing possono avvenire anche attraverso i social network e altre comunità online.[18]

Tipo di attacco
Attacco di phishing

Debolezza/Vulnerabilità:
Errore umano – l'incautela o l'ignoranza della vittima ha portato alla minaccia informatica.

Che cosa è successo?
Ignoti criminali informatici sono riusciti a risalire al contatto e-mail del dipendente vittima dell'attacco che chiedeva di aggiornare le credenziali di accesso a Office 365 Teams (la piattaforma online utilizzata in azienda).

18 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

Figura 1: Posta elettronica.

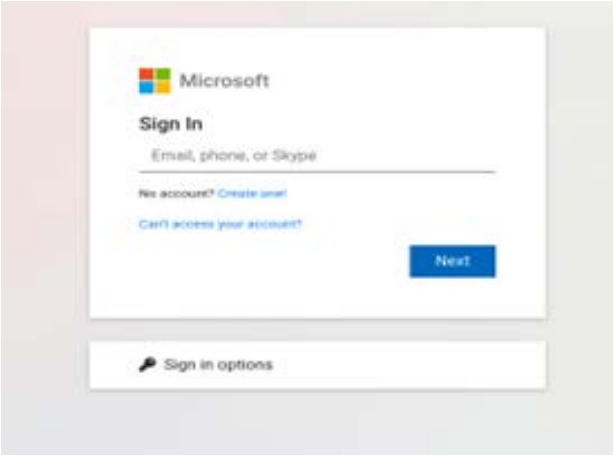


Figura 2: Microsoft Log-In.

La vittima ha cliccato sul falso link incluso nella mail inviata dai criminali informatici e ha inserito i dati di accesso al suo account aziendale.

Come è stato notato?

Il Computer Emergency Response Team (CERT) dell'azienda ha rilevato alcuni accessi sospetti da altri Paesi come Regno Unito, Algeria e Stati Uniti, mentre la vittima era solita collegarsi da Milano, Lombardia, Italia. Ciò ha destato il sospetto e la diffidenza del CERT.

Quali misure sono state adottate?

- Il CERT ha chiesto alla vittima di confermare se avesse effettuato l'accesso al suo account da quei paesi. La vittima ha negato, quindi il CERT gli ha chiesto di cambiare le sue credenziali di accesso.
- Poste Italiane ha introdotto un efficace sistema di monitoraggio che opera a livello nazionale. In generale, il software di posta elettronica aziendale è dotato di un Firewall, ovvero un filtro antispam che intercetta e blocca la maggior parte delle e-mail dannose.

Qual è il risultato delle misure di difesa?

Quando una di queste e-mail di spam riesce a superare il filtro, i dipendenti hanno a disposizione un pulsante nella loro casella di posta elettronica per segnalare la suddetta e-mail direttamente al CERT. Una volta che il CERT ha analizzato l'e-mail e l'ha classificata come dannosa, estrae le informazioni e i link che contiene e li inserisce nei controlli perimetrali, bloccando l'accesso al link.

Caso 2 – Attacco alla catena di fornitura

Titolo	Attacco alla catena di approvvigionamento
Fonte	ERG Evolving Energies - Azienda energetica italiana
Periodo di riferimento	Agosto 2021
Tag	Azienda, attacco al server, furto di dati, malware, ransomware
Stato	Risolto entro la settimana in cui si è verificato tramite la modifica delle credenziali di accesso
Applicabilità Escape Room	Non trasferibile: Le informazioni divulgate da ERG sul modo in cui gli esperti di CS hanno agito nella gestione dell'attacco hacker non sono dettagliate. Pertanto, sarebbe difficile creare la narrazione del caso, soprattutto perché mancano i principali aspetti tecnici dell'attacco.

Eyes on ransomware:
Un attacco Ramsomware è un malware che utilizza la crittografia per chiedere un riscatto per le informazioni della vittima. I dati critici di un utente o di un'organizzazione vengono crittografati in modo da non poter accedere a file, database o applicazioni. Viene quindi richiesto un riscatto per fornire l'accesso.
Nel caso dei Ransomware, le aziende hanno opzioni limitate

- pagare il riscatto
- decriptare i dati rubati
- perdere/diffondere pubblicamente i dati rubati.

Tipo di attacco
Ransomware

Debolezza/Vulnerabilità:
Nel caso dei Ransomware non è possibile individuare un "errore umano", perché si tratta di attacchi mirati perpetrati contro aziende i cui sistemi di protezione sono stati monitorati e studiati nel tempo dagli autori del reato.

Che cosa è successo?
ERG è il primo operatore eolico italiano e tra i primi dieci operatori onshore del mercato europeo. Il Gruppo opera nei settori dell'energia eolica, solare, idroelettrica e della

cogenerazione termoelettrica ad alto rendimento. ERG si affida a Engineering Ingegneria Informatica per i servizi di sicurezza informatica.

- Secondo la ricostruzione della stampa, il 30 Luglio 2021 la banda del ransomware LockBit 2.0 ha colpito Engineering Ingegneria Informatica riuscendo a infettare i suoi server con un virus che avrebbe compromesso le credenziali di accesso ad alcune VPN dei suoi clienti, tra cui quella di ERG.
- Engineering Ingegneria Informatica ha segnalato l'attacco ai propri clienti e ha avviato approfonditi audit, attraverso i quali, nella notte del 5 Agosto, ha rilevato la matrice e l'entità dell'attacco, nonché le aziende violate a loro volta. L'attacco è stato condotto da un ransomware noto come RansomEXX, che è passato attraverso Engineering Ingegneria Informatica fino a raggiungere il sistema informatico di ERG.
- Appena entrati nel sistema, i criminali informatici hanno copiato una parte dei file dell'azienda procedendo alla loro crittografia. I criminali hanno ricattato pubblicamente ERG condividendo il messaggio sottostante sulla homepage del sito web di ERG, minacciando l'azienda di divulgare i dati rubati entro pochi giorni se non avesse pagato un riscatto. Lo scopo principale degli attacchi di hacking è infatti quello di rubare i dati come leva per i tentativi di estorsione.

Come è stato notato?

Durante l'attacco, ERG ha subito alcune limitate interruzioni della sua infrastruttura di tecnologia dell'informazione e della comunicazione (TIC).

Quali misure sono state adottate?

- Attivazione immediata delle procedure interne di cybersecurity: ERG non ha condiviso informazioni dettagliate sulle azioni tecniche intraprese per far fronte ai danni causati dall'attacco. L'unica informazione certa disponibile è che la società di CS incaricata ERG, Engineering Ingegneria Informatica, ha chiesto all'azienda di cambiare le credenziali di accesso agli account.
- In seguito, ERG ha confermato che tutte le strutture erano correttamente funzionanti e non avevano subito interruzioni, garantendo così l'operatività aziendale.
- Per impedire ai criminali informatici di accedere ulteriormente ai dati aziendali, Engineering Ingegneria Informatica ha invitato ERG a modificare le password degli account supportati dai suoi team e a segnalare qualsiasi altro sospetto di utilizzo inappropriato delle sue credenziali.

Qual è il risultato delle misure di difesa?

A causa dell'entità limitata del danno, ERG si è rifiutata di pagare il riscatto. Secondo la dichiarazione di ERG, gli hacker avevano criptato dati ritenuti piuttosto irrilevanti.

Caso 3 – Attacco di negazione del servizio (DoS- Denial of Service)

Titolo	Attacco di negazione del servizio (DoS-Denial of Service)
Fonte	Società di noleggio online (Italia)
Periodo di riferimento	Ottobre 2021
Tag	PMI, Azienda, Furto di dati, Denial-of-Service (DOS)
Stato	Risolto entro la settimana in cui si è verificato, chiudendo la piattaforma online e creandone una nuova.
Applicabilità Escape Room	Trasferibile con difficoltà: pur essendo un caso comune, le sue conseguenze non sono perfettamente replicabili.

Eyes on DoS:
Gli attacchi DOS funzionano inondando di traffico sistemi, server e/o reti per sovraccaricare le risorse e la larghezza di banda. Il risultato è che il sistema non è in grado di elaborare e soddisfare le richieste legittime. Oltre agli attacchi denial-of-service (DoS), esistono anche attacchi distributed denial-of-service (DDoS).
Gli attacchi DoS saturano le risorse di un sistema con l'obiettivo di impedire la risposta alle richieste di servizio. D'altra parte, un attacco DdoS viene lanciato da più macchine host infette con l'obiettivo di ottenere la negazione del servizio e mettere offline un sistema, aprendo così la strada a un altro attacco per entrare nella rete/ambiente.[19]

Tipo di attacco
Negazione del servizio (DoS)

Debolezza/Vulnerabilità
Errore umano – Il capo dell'azienda è stato mal consigliato.

Che cosa è successo?
- Prima che si verificasse il problema, l'azienda presentata si era affidata occasionalmente a Sync Security (SS), una società privata di Cyber Security specializzata in protezione dei dati, conformità e continuità aziendale. Quattro mesi prima dell'attacco, SS ha rilevato sulla piattaforma online "Shutdown" che l'azienda in questione era classificata tra le prime 100 aziende più vulnerabili agli attacchi informatici.

19 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

- Piattaforme come "Shutdown" riportano dati - raccolti nel tempo da spider web - che indicano il tipo e il livello di vulnerabilità dei domini delle aziende e spiegano i modi in cui tali vulnerabilità possono essere sfruttate. Queste piattaforme sono facilmente accessibili a tutti, esponendo così ancora di più le aziende che si classificano tra le prime cento.
- È infatti statisticamente provato che si subisca un attacco informatico entro i primi 12 mesi dalla pubblicazione di tali file. Poiché gli attacchi perpetrati sulla base delle informazioni divulgate da queste piattaforme non sono mirati (negli attacchi non mirati, gli aggressori prendono di mira indiscriminatamente il maggior numero possibile di dispositivi, servizi o utenti. Non si preoccupano di chi sia la vittima, perché ci sarà un certo numero di macchine o servizi con vulnerabilità[20]), quindi è possibile per le aziende difendersi dalle minacce informatiche e prevenire perdite economiche o di dati.
- Il SOC (Security Operation System) di Sync Security ha quindi segnalato questo rischio al responsabile dell'azienda, che però ha sottovalutato il problema e si è rifiutato di ricorrere a misure di difesa preventive.
- Quattro mesi dopo, il sito web dell'azienda, nella sezione di interazione con i clienti basata su moduli, ha subito un primo DOS: ignoti criminali informatici, provenienti da un paese europeo non specificato, sono riusciti a bloccare il sito web, impedendone la produttività.

Come è stato notato?

In breve tempo, gli attacchi sono diventati più mirati e profondi, con la conseguente compromissione dei dati commerciali e personali dei clienti. Pertanto, il responsabile dell'azienda ha richiesto l'intervento degli esperti di Sync Security.

Quali misure sono state adottate?

- L'intervento è stato immediato: Gli esperti di Sync Security hanno messo in atto misure di contenimento. Nel giro di 3-4 ore l'attacco è diventato ancora più aggressivo, per cui le misure messe in atto non erano più sufficienti a contenere i danni.
- Gli esperti di Sync Security, su autorizzazione dell'amministratore delegato dell'azienda, hanno preso la drastica decisione di bloccare l'accesso al sito per gli utenti al di fuori dell'Italia.
- Nel frattempo il problema - un errore legato al codice del sito - è stato risolto e sono stati messi in atto presidi anti-DOS. Inoltre, nei giorni successivi, gli esperti di Sync Security hanno utilizzato una piattaforma per monitorare il rating IP di ogni utente.

Qual è il risultato delle misure di difesa?

- Chiudere il sito web e riaprirlo una volta neutralizzata la minaccia.
- La chiusura del sito web da parte di Google attraverso la società di hosting ha comportato la scomparsa dell'azienda e della sua piattaforma di noleggio dai browser. Pertanto, l'azienda ha dovuto intraprendere campagne promozionali, attività di marketing e DEM (Direct Email Marketing) che hanno ulteriormente appesantito il bilancio delle perdite.

20 National Cyber security center, https://www.ncsc.gov.uk/information/how-cyber-attacks-work, accessed on Juanuary 20 2023.

Lezioni apprese:
Dopo questa esperienza, l'azienda ha deciso di investire lo 0,5% del fatturato nella sicurezza informatica, stipulando un contratto con Sync Security.

Caso 4 – SQL injection

Titolo	SQL injection
Fonte	Compagnia di assicurazioni (Italia)
Periodo di riferimento	Ottobre 2021
Tag	PMI, Azienda, Furto di informazioni di pagamento, SQL injection
Stato	Risolto entro la fine di novembre 2021 dopo un audit tecnico.
Applicabilità Escape Room	Non trasferibile: Le informazioni su come gli esperti di CS hanno agito nella gestione dell'attacco hacker non sono dettagliate. Pertanto, sarebbe difficile creare una narrazione del caso, soprattutto perché si è trattato di un falso allarme.

Eyes on SQL:
Ciò si verifica quando un aggressore inserisce codice dannoso in un server utilizzando il linguaggio di interrogazione del server (SQL), costringendo il server a fornire informazioni protette. Questo tipo di attacco di solito comporta l'invio di codice dannoso nei commenti o nella casella di ricerca di un sito web non protetto. Le pratiche di codifica sicure, come l'uso di istruzioni preparate con query parametrizzate, sono un modo efficace per prevenire le iniezioni SQL.
Quando un comando SQL utilizza un parametro invece di inserire direttamente i valori, può consentire al backend di eseguire query dannose. Inoltre, l'interprete SQL utilizza il parametro solo come dato, senza eseguirlo come codice.[21]

21 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

Tipo di attacco
SQL injection

Debolezza/ Vulnerabilità
Errore umano: l'utente del sito web ha prodotto un rapporto tecnicamente impreciso.

Che cosa è successo?
Nei mesi precedenti l'attacco, l'Agenzia di Sicurezza Informatica incaricata dall'azienda ha eseguito diversi test per valutare il livello di sicurezza del sistema aziendale. Sebbene questi test di sicurezza siano stati condotti in modo approfondito, mentre l'azienda stava conducendo una promozione di vendita, ha ricevuto una segnalazione da un'organizzazione di consumatori, che ha finito per bloccare la campagna.

Come è stato notato?
Un membro dell'organizzazione dei consumatori ha dichiarato di aver perso il proprio denaro mentre inseriva i dati di pagamento sul sito web dell'azienda.

Quali misure sono state adottate?
- Il legale dell'azienda ha suggerito al responsabile di mettere offline il sito web. Si è pensato che si trattasse di un caso di SQL injection, presumibilmente un cybercriminale ha inserito un codice maligno nel server dell'azienda utilizzando il Server Query Language (SQL), costringendo così il server a fornire informazioni protette.
- Il responsabile dell'azienda ha chiesto spiegazioni all'Agenzia di Sicurezza Informatica: come è stato possibile che proprio dopo un test di verifica preliminare l'azienda abbia subito un attacco informatico? Tanto più che per questo tipo di Agenzie, gli attacchi informatici come le iniezioni SQL sono abbastanza facili da individuare.
- L'Agenzia di Sicurezza Informatica ha agito immediatamente, conducendo anche - in privato - un'analisi passiva del rapporto.
- Il cliente che ha dichiarato di aver perso il proprio denaro inserendo i dati di pagamento sul sito web dell'azienda era uno studente universitario di ingegneria informatica che, nonostante avesse una certa conoscenza dell'argomento, è stato tratto in inganno dal fatto di aver letto "injection" all'interno del codice sorgente HTML del sito web dell'azienda, quando invece si trattava solo di una caratteristica del linguaggio di programmazione Java.

Qual è il risultato delle misure di difesa?
- Le analisi statiche del programma hanno stabilito che l'attacco non si è mai verificato. Pertanto, il furto subito dall'utente non era legato al sito web dell'azienda. Sebbene fosse improbabile che un sistema sottoposto a pressure test solo di recente presentasse una vulnerabilità, questa doveva essere verificata ufficialmente tramite audit tecnico.
- L'aver messo offline il sito web stava costando all'azienda una forte perdita di fatturato.

Lezioni apprese:
In questo caso non si tratta tanto di un errore, quanto di un merito. L'azienda - per quanto piccola - affidando a un professionista della sicurezza informatica l'esecuzione di test di sicurezza, si è dimostrata previdente. Infatti, l'investimento fatto sulla sicurezza informatica, ha aiutato quest'ultima a prevenire il rischio di una forte perdita di profitti. Infatti, avendo avuto dei professionisti a cui affidarsi, il sito web aziendale è stato rimesso in funzione immediatamente dopo l'esito dell'analisi tecnica effettuata in poche ore. Al contrario, senza prevenzione, questa segnalazione fatta dall'utente, che alla fine si è rivelata inesatta, sarebbe costata all'azienda il triplo in termini di mancati profitti, oltre al costo del pronto intervento degli specialisti di CS.

Caso 5 – Smishing

Titolo	Smishing
Fonte	Piccola impresa al dettaglio
Periodo di riferimento	Marzo 2021
Tag	Imprese, furto d'identità, attacco via SMS, Phishing, Smishing
Stato	Risolto entro la fine di marzo 2021 con la modifica delle credenziali di accesso.
Applicabilità Escape Room	Altamente trasferibile: Si tratta di un caso comune che può essere facilmente compreso e trasferito nel modello dell'escape room.

Eyes on phishing e smishing:
Lo smishing è una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco. Il criminale esegue l'attacco con l'intento di raccogliere informazioni personali, compresi i numeri di assicurazione sociale e/o di carta di credito. Lo smishing viene attuato tramite messaggi di testo o SMS, dando all'attacco il nome di "SMiShing". Quando i criminali informatici effettuano il "phishing", inviano e-mail fraudolente che cercano di indurre il destinatario a cliccare su un link dannoso. Lo smishing utilizza semplicemente i messaggi di testo al posto delle e-mail. In sostanza, questi criminali informatici vogliono rubare i vostri dati personali, che possono poi utilizzare per commettere frodi o altri crimini informatici.

Tipo di attacco
Smishing

Debolezza/Vulnerabilità
Errore umano: la vittima è caduta in una trappola. Non si è reso conto che la banca era già in possesso dei suoi dati personali, quindi non c'era motivo di chiedere al cliente di compilare un modulo. Il cliente ovviamente non sapeva che una banca non chiederebbe mai a un cliente di compilare moduli/login via e-mail.

Che cosa è successo?
- Gli ignoti criminali informatici sono riusciti a risalire al numero personale del dipendente vittima dell'attacco. La vittima aveva richiesto la surroga del mutuo, cioè aveva avviato il processo di trasferimento del mutuo da una banca all'altra, ma stava ancora aspettando che la vecchia banca gli inviasse tutti i documenti necessari.
- La vittima ha ricevuto un SMS che la informava che i suoi documenti erano stati caricati sul suo conto di mobile banking e le chiedeva di cliccare su un link per procedere al download dall'area personale del sito web della banca. La vittima ha utilizzato il computer aziendale per eseguire questa procedura, per scaricare e stampare i documenti in ufficio. Ha cliccato sul link ed è stato reindirizzato a un sito web, una copia perfetta di quello originale, per cui non si è preoccupata di controllare l'URL del sito. Le è quindi stato chiesto di compilare un modulo con i suoi dati personali: Nome, cognome, numero di telefono, codice fiscale.
- Una volta fatto, è apparsa la notifica "abbiamo inviato i tuoi documenti", che questa volta chiedeva di cliccare sul link e di inserire le credenziali di accesso. Nonostante la vittima fosse sicura di aver inserito le credenziali giuste, la password era "sbagliata". La pagina che apparentemente era stata appena aggiornata era la vera pagina della banca.
- I criminali hanno rubato le credenziali di accesso alla banca e quindi hanno avuto accesso ai dati personali della vittima. Utilizzando le credenziali sono riusciti a superare il sistema di autenticazione multifattoriale, permettendo loro di controllare il dispositivo mobile token e di autorizzare i bonifici bancari direttamente dall'area personale del sito web della banca.

Come è stato notato?
Dopo qualche ora, quando la vittima ha effettuato l'accesso all'app mobile della banca con il suo smartphone, si è subito accorta di avere un saldo del conto inferiore.

Quali misure sono state adottate?
- La vittima ha cambiato le credenziali di accesso e ha comunicato all'istituto bancario di essere stato vittima di una campagna di phishing.
- Ha riferito dell'attacco anche all'interno dell'azienda. L'azienda ha incaricato uno specialista di cybersecurity di condurre un'analisi approfondita del sistema per verificare se uno dei link su cui la vittima aveva fatto clic avesse scaricato malware o qualsiasi altra minaccia al database aziendale. L'analisi tecnica non ha rilevato alcun virus: i dati aziendali erano al sicuro.

Qual è il risultato delle misure di difesa?

La situazione è stata risolta cambiando le credenziali di accesso. Tuttavia, la vittima non è riuscita a recuperare il denaro. Avrebbe dovuto contattare la banca per accertarsi della veridicità di quell'SMS. Inoltre, non avrebbe dovuto utilizzare il computer aziendale per sbrigare questioni personali, anche se urgenti. In questo caso va considerato anche l'aspetto psicologico della situazione: i mutui sono questioni delicate, quindi è anche comprensibile che la vittima abbia sentito l'urgenza di sbrigare le pratiche non appena ha ricevuto un SMS – in questo caso malevolo – a questo proposito.

Caso 6 – Spam phishing

Titolo	Spam phishing
Fonte	Organismo governativo
Periodo di riferimento	2018
Tag	Ente governativo, Furto d'identità, Social Engineering, Attacco via e-mail, Phishing
Stato	Risolto per modifica delle credenziali di accesso
Applicabilità Escape Room	Trasferibile con difficoltà: Si tratta di una campagna di phishing molto sofisticata, per cui sarebbe difficile riprodurre alcuni elementi.

Eyes on Social Engineering :
La tecnica di attacco di social engineering consiste nella manipolazione psicologica per indurre gli utenti a commettere errori di sicurezza o a fornire informazioni sensibili. In questo caso, gli ignoti criminali informatici hanno prima indagato sulle vittime designate per raccogliere le informazioni di base necessarie, come i potenziali punti di accesso e i protocolli di sicurezza deboli, per procedere con l'attacco.

Tipo di attacco

Spam phishing

Debolezza/Vulnerabilità

Errore umano – social engineering. Le vittime sono cadute in una truffa molto sofisticata, accuratamente dettagliata e sviluppata nel tempo. Quando i criminali informatici mettono in atto processi per fidelizzare le vittime, è molto difficile distinguere le e-mail dannose da quelle veritiere. Questo è uno dei principali rischi associati al social engineering, che fa leva sulle debolezze delle vittime, in questo caso una ricompensa psicologica legata a una passione, per estorcere informazioni sensibili.

Che cosa è successo?

- Al momento dell'attacco, le e-mail dei dipendenti di questo ente governativo erano generate nello stesso modo: nome + cognome + dominio. In questo modo, le informazioni dei titolari degli indirizzi e-mail non venivano oscurate, poiché non erano considerate dati sensibili.
- In questo modo è stato più facile per i criminali risalire all'identità di un gruppo di dipendenti. Gli autori hanno iniziato a spiare i profili social - Instagram, Facebook, Twitter, LinkedIn - di questi dipendenti e, osservando le foto e i video postati, le pagine seguite e i follower, hanno individuato una passione comune a circa 20 dipendenti: il bodybuilding. Inizia così una campagna di phishing molto sofisticata.
- In un primo momento, i criminali hanno avviato un'attività di phishing di prova: hanno inviato e-mail vuote alle vittime per vedere chi fosse più propenso a cadere nella trappola. In seguito, questi dipendenti hanno ricevuto un'e-mail relativa a un nuovo accordo tra l'ente governativo e un famoso marchio di integratori per l'allenamento, in occasione del quale questo marchio stava lanciando una campagna di vendita. Inserendo i propri dati di acquisto e di spedizione nel link presente nell'e-mail, avrebbero aderito a questa campagna di vendita, ricevendo i prodotti a casa loro a un prezzo molto speciale. Di questi 20 dipendenti solo due sono stati ingannati.
- Cliccando sul link, sono stati reindirizzati alla - falsa - pagina di accesso dell'ente governativo, dove "trattandosi di una promozione riservata esclusivamente ai dipendenti di quell'ente governativo", è stato richiesto loro di accedere con le proprie credenziali di accesso: nome utente e password.
- Una volta "finalizzato" il pagamento sul sito web del marchio FAKE - in cui era disponibile anche un numero di assistenza clienti - i criminali mettevano in atto un processo per trattenere la vittima, inviando la merce acquistata. I criminali si sono assicurati di rendere plausibile la spedizione, curando ogni dettaglio, come l'imballaggio, le etichette, ecc.
- Dopo aver ricevuto la merce acquistata, le due vittime hanno sparso la voce tra i colleghi sulla presunta veridicità di questa campagna di vendita. In questo modo, il link malware risultante dalla campagna di phishing ha iniziato a circolare tra i dipendenti - a diversi livelli - e in pochi giorni ben 300 persone sono cadute nella trappola.

Come è stato notato?

Solo quando un superiore è venuto a conoscenza di quanto stava accadendo, sapendo che c'era un accordo con questo marchio, ha capito che il personale era stato vittima di una truffa. I dipendenti non solo hanno incautamente fornito le loro informazioni personali e i dettagli dei pagamenti, ma hanno anche esposto a rischio l'ente per cui lavorano, che in quanto governo possiede un numero enorme di dati personali dei cittadini, il cui utilizzo per scopi malevoli potrebbe essere innumerevole.

Quali misure sono state adottate?

- Per ridurre i tempi, tutti gli account delle vittime della truffa sono stati bloccati e le password sono state successivamente modificate.
- Oggi il governo ha proceduto a sostituire anche i nomi utente.

Qual è il risultato delle misure di difesa tecniche / organizzative / sociali?

- La situazione è stata risolta cambiando le password e gradualmente i nomi utente.
- Oggi, a quattro anni dall'attacco, tutti gli indirizzi e-mail sono stati cambiati: non è più possibile risalire all'identità dei titolari degli indirizzi e-mail, poiché nome e cognome sono stati sostituiti da un codice.

5.2 Casi di sicurezza informatica dalla Germania

Caso 1 – E-mail di spam

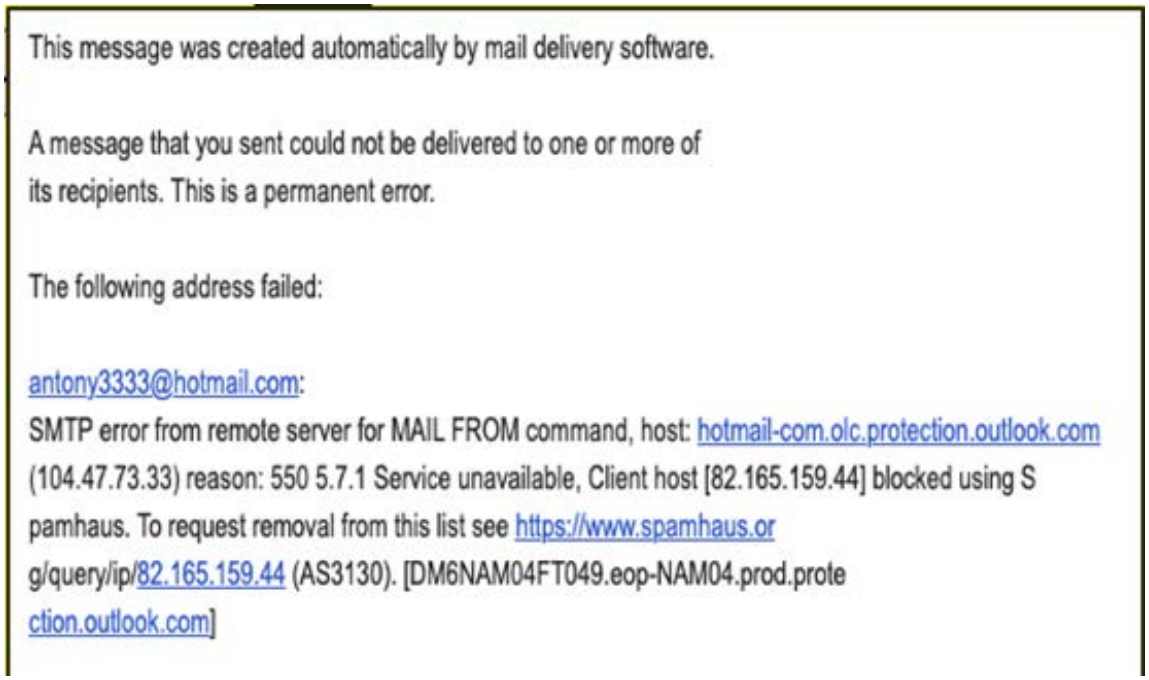
Titolo	E-mail di spam
Fonte	Consulenza in tecnologia dei media, tedesco/ PMI locale di Bielefeld
Periodo di riferimento	Marzo 2022
Tag	PMI, furto d'identità, attacco via e-mail, truffa
Stato	Risolto il 25.3.22 per modifica della password
Applicabilità Escape Room	Facilmente trasferibile: Il caso semplice è facile da comprendere e può essere trasferito a un modello di Escape Room limitato.

Eyes On furto d'identità
Il furto d'identità è il reato che consiste nell'ottenere le informazioni personali o finanziarie di un'altra persona per utilizzarne l'identità al fine di commettere frodi, come ad esempio effettuare transazioni o acquisti non autorizzati. Il furto d'identità viene commesso in molti modi diversi e le vittime subiscono danni al credito, alle finanze e alla reputazione.

Tipo di attacco
Furto d'identità

Debolezza/Vulnerabilità:
Errore umano – Password troppo semplice o non modificata di recente.

Che cosa è successo?
Il criminale informatico ha ottenuto la password dell'account della vittima. Da questo account ha poi inviato e-mail di spam, presumibilmente in gran numero, a indirizzi sconosciuti alla vittima.



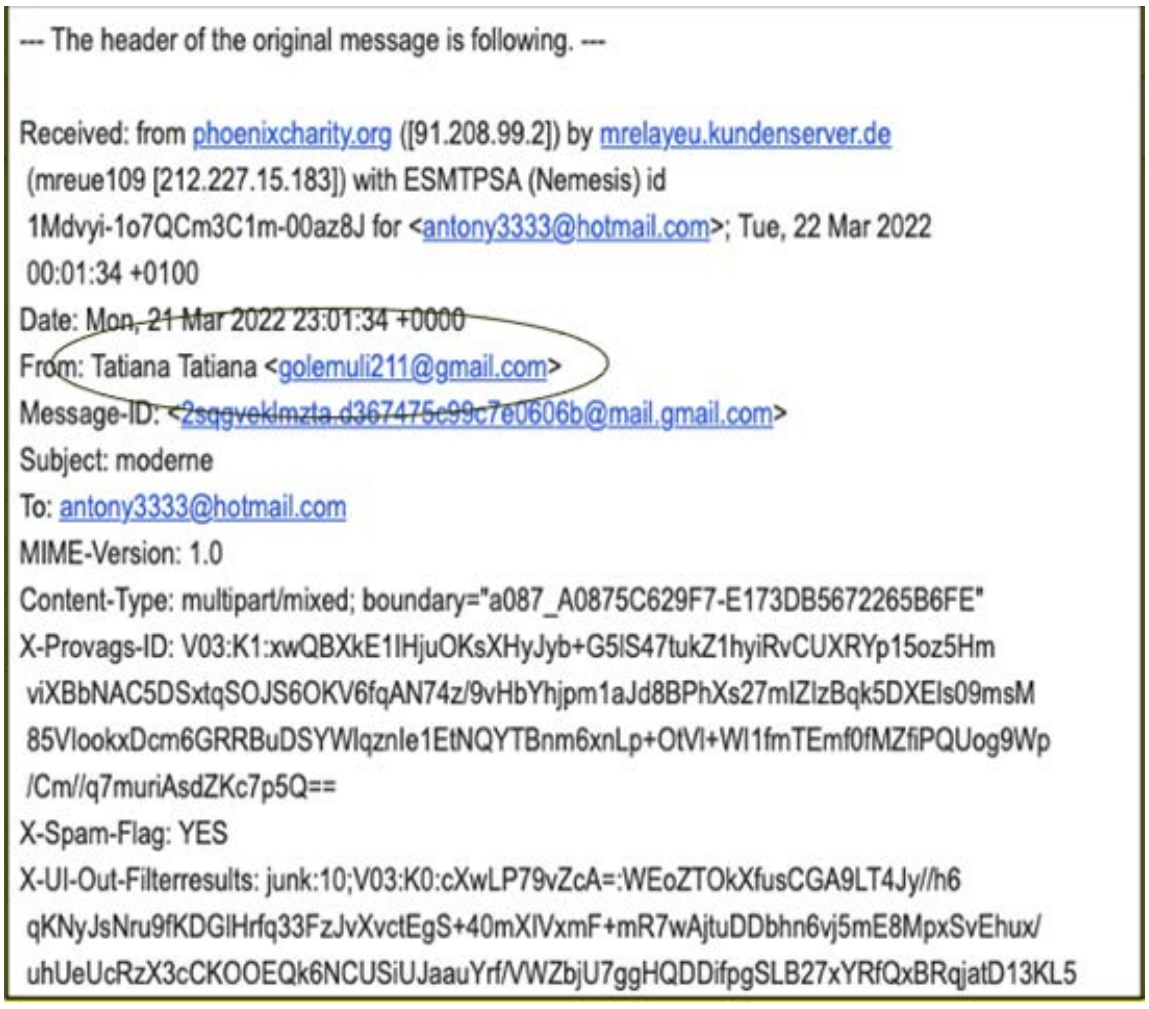
This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its recipients. This is a permanent error.

The following address failed:

antony3333@hotmail.com:
SMTP error from remote server for MAIL FROM command, host: hotmail-com.olc.protection.outlook.com (104.47.73.33) reason: 550 5.7.1 Service unavailable, Client host [82.165.159.44] blocked using S pamhaus. To request removal from this list see https://www.spamhaus.or g/query/ip/82.165.159.44 (AS3130). [DM6NAM04FT049.eop-NAM04.prod.prote ction.outlook.com]

Figura 3: Notifica di errore da parte del server di posta elettronica ricevente.



--- The header of the original message is following. ---

Received: from phoenixcharity.org ([91.208.99.2]) by mrelayeu.kundenserver.de (mreue109 [212.227.15.183]) with ESMTPSA (Nemesis) id 1Mdvyi-1o7QCm3C1m-00az8J for <antony3333@hotmail.com>; Tue, 22 Mar 2022 00:01:34 +0100
Date: Mon, 21 Mar 2022 23:01:34 +0000
From: Tatiana Tatiana <golemuli211@gmail.com>
Message-ID: <2sqgveklmzta.d367475c99c7e0606b@mail.gmail.com>
Subject: moderne
To: antony3333@hotmail.com
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="a087_A0875C629F7-E173DB5672265B6FE"
X-Provags-ID: V03:K1:xwQBXkE1lHjuOKsXHyJyb+G5lS47tukZ1hyiRvCUXRYp15oz5Hm viXBbNAC5DSxtqSOJS6OKV6fqAN74z/9vHbYhjpm1aJd8BPhXs27mlZlzBqk5DXEls09msM 85VlookxDcm6GRRBuDSYWlqznle1EtNQYTBnm6xnLp+OtVl+Wl1fmTEmf0fMZfiPQUog9Wp /Cm//q7muriAsdZKc7p5Q==
X-Spam-Flag: YES
X-UI-Out-Filterresults: junk:10;V03:K0:cXwLP79vZcA=:WEoZTOkXfusCGA9LT4Jy//h6 qKNyJsNru9fKDGlHrfq33FzJvXvctEgS+40mXlVxmF+mR7wAjtuDDbhn6vj5mE8MpxSvEhux/ uhUeUcRzX3cCKOOEQk6NCUSiUJaauYrf/VWZbjU7ggHQDDifpgSLB27xYRfQxBRqjatD13KL5

Figura 4: Intestazione della mail di spam.

- Secondo la Figura 3, questa email è stata bloccata dal server di posta ricevente in base al rilevamento dello spam. Si può presumere che un numero elevato di e-mail di spam inviate automaticamente dall'account della vittima abbia raggiunto gli indirizzi specificati dall'aggressore. Questo è l'impatto principale dell'attacco. Si possono fare solo ipotesi sui contenuti inviati.
- Ulteriori ricerche su[22] hanno scoperto che spesso le e-mail di spam/scam con l'indirizzo di ritorno golemuli211@gmail.com distribuiscono il contenuto illustrato nella Figura 4. Va notato che il truffatore non ha utilizzato l'indirizzo di ritorno della vittima.
- Il danno sembra quindi essere limitato all'invio di spam/scam dall'account della vittima. Non è stato richiesto denaro alla vittima.

Come è stato notato?

Il provider di posta elettronica della vittima ha ovviamente riconosciuto l'abuso dell'account e ha inviato alla vittima il seguente avviso (cfr. fig. 4). Allo stesso tempo, la vittima dell'attacco ha notato che le e-mail apparentemente inviate dal suo account venivano rifiutate dai server di posta ricevuti. Il numero di queste e-mail era molto elevato, circa 200.

Quali misure sono state adottate?

Misura: Passaggio a una password più sicura

Per risolvere il problema in questione abbiamo condotto le seguenti verifiche e misure:

- **Controllo 1: le e-mail sono state inviate all'insaputa degli utenti?**
  - Controllare i dispositivi finali (PC, smartphone o tablet) con un antivirus aggiornato.
  - Aggiornare il software sui dispositivi finali degli utenti e attivare gli aggiornamenti automatici.
  - Utilizzare il firewall del router, del PC o del software di sicurezza Internet.
  - Se il virus è stato trovato e rimosso con successo, cambiate le vostre password.
- **Controllo 2: l'utente ha inviato la mail di proposito?**
  - Verificare se il software di posta elettronica in uso è configurato correttamente.
- Assicurarsi che gli indirizzi dei destinatari siano raggiungibili, mantenendo regolarmente le mailing list degli utenti.
- Se l'utente invia newsletter o altri invii di massa, deve prestare attenzione ai seguenti standard:
  - Il mittente ha ottenuto il consenso del destinatario (double opt-in)?
  - La newsletter contiene un link che permette al destinatario di annullare l'iscrizione con un solo clic (opt-out)
  - I destinatari della posta elettronica per i quali l'utente riceve un messaggio non recapitabile vengono automaticamente eliminati dal database degli indirizzi (gestione dei bounce).

Qual è il risultato delle misure di difesa?

- In questo caso la password dell'e-mail è stata modificata dalla vittima in un breve lasso di tempo.
- Il blocco è stato rimosso automaticamente dal provider nel giro di pochi minuti.

22 https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727

Caso 2 – Installazione del software Crypto Miner

Titolo	Il software Crypto Miner è stato installato
Fonte	Cliente non rivelato/Germania
Periodo di riferimento	Giugno 2019
Tag	PMI, crypto miner, crypto jacking, truffa
Stato	Risolto
Applicabilità Escape Room	Altamente trasferibile:Il caso semplice è facile da capire

Eyes On Crypto Miner:
Il Crypto Miner è un processo di creazione di nuove "monete" digitali. Tuttavia, la semplicità non si ferma qui. Il processo di recupero di queste monete richiede la risoluzione di complessi puzzle, la convalida delle transazioni di criptovaluta su una rete blockchain e l'aggiunta a un registro distribuito per individuarle.

Tipo di attacco
Installazione software Crypto Miner

Debolezza/Vulnerabilità:
Errore umano – Il download e l'installazione di software open-source da Internet è stato il fattore scatenante di questo attacco. Non è stato scaricato da siti "sicuri" o "ufficiali" del produttore.

Che cosa è successo?
- Presso la sede di un cliente sono stati installati dei Crypto Miners a seguito di un download arbitrario di software da parte dei dipendenti. Quando i Crypto Miners sono stati disinstallati, è iniziata la crittografia della struttura di rete (server, client, backup, copie shadow, ecc.). A ciò è seguita un'estorsione del cliente.
- I dipendenti del cliente avevano diritti di amministrazione locale e potevano installare software sui client. Di conseguenza, si erano installati anche i Crypto Miners.
- I Crypto Miners hanno iniziato a lavorare subito dopo l'installazione e hanno utilizzato tutte le risorse del client per il mining.

Come è stato notato?

Le prestazioni dei client peggioravano sempre di più. I processi semplici richiedevano molto tempo. Inoltre, l'utilizzo della CPU e della RAM era costantemente al 99%.

Quali misure sono state adottate?

- La struttura di rete è stata scollegata da Internet
- I client e i server sono stati rimossi dalla rete
- L'intera infrastruttura tecnica è stata reinstallata
  - Protezione antivirus uniforme, backup memorizzati esternamente, revoca dei diritti di amministrazione agli utenti.
  - È stato installato un sistema firewall.

Qual è il risultato delle misure di difesa?

- Grazie alle misure di sicurezza implementate, non si sono verificate nuove contaminazioni virtuali.
- Il malware già scaricato è stato rimosso dal sistema di protezione antivirus prima che potesse essere eseguito.
- Durante la disinstallazione, il software ha avviato la crittografia della struttura di rete. In questo caso, tutti i dispositivi disponibili sulla rete sono stati crittografati.
- I backup e le copie shadow sono stati cancellati e non è stato possibile ripristinarli. Le operazioni del cliente sono state stato bloccato dal 31.12.18 al 01.07.19
- I dati dovevano essere gestiti manualmente. Non c'è stata risposta all'estorsione.
- L'infrastruttura è stata reinstallata e parzialmente ripristinata dai vecchi backup esistenti.

Lezioni apprese:
Questo tipo di attacco può ripetersi. Tuttavia, è possibile prevenirlo grazie a una protezione antivirus uniforme e aggiornata con moduli aggiuntivi come Intercept X o una Sandbox. Inoltre, i diritti di amministrazione possono essere revocati agli utenti, in modo che non sia possibile installare qualsiasi software.

Caso 3 – Mail/attacco di phishing

Titolo	Mail di phishing/attacco
Fonte	Cliente non rivelato / Germania
Periodo di riferimento	Febbraio 2022
Tag	PMI, phishing, frode
Stato	Risolto
Applicabilità Escape Room	Facilmente trasferibile: Il caso semplice è facile da capire e può essere trasferito a un modello di Escape Room limitato. Poiché si tratta di un caso standard che si verifica molto spesso, non è molto interessante per il modello.

Tipo di attacco
Phishing

Debolezza/Vulnerabilità:
Errore umano - il nome utente e la password del cliente per l'online banking sono stati inseriti seguendo il link di una mail di phishing e trasmessi all'autore del phishing.

Che cosa è successo?
A un cliente sono state inviate e-mail di phishing con termini e condizioni aggiornati o modifiche dei costi. Successivamente, è stato necessario effettuare il login all'online banking per visualizzare le modifiche.

Come è stato notato?
È stato contattato l'amministratore informatico interno della società segnalante. Ha analizzato e controllato la posta.

Quali misure sono state adottate?
- Il dominio di posta è stato bloccato dal firewall.
- Tuttavia, circa 3.000 euro sono stati trasferiti su un altro conto bancario a causa di questa frode. Attualmente il rimborso da parte della banca è ancora in sospeso.

Qual è il risultato delle misure di difesa tecnica / organizzativa / sociale?

- È stata effettuata una formazione ai dipendenti in materia di consapevolezza.
- I dipendenti hanno ricevuto un "foglio informativo" su come riconoscere le e-mail di phishing. In seguito, le e-mail di phishing non sono più state cliccate e sono state cancellate direttamente.

Lezioni apprese:
Questo tipo di attacco può ripetersi in qualsiasi momento. Per tutelarsi è possibile utilizzare domini di posta ufficiali come Gmail o simili. Se li si blocca, tra l'altro, le e-mail "ufficiali/corrette" non arriveranno più. Inoltre, i link vengono rigenerati a ogni attacco. In questo caso il blocco fornisce solo una protezione temporanea.

Caso 4 -Mail/Attacchi di phishing

Titolo	Mail di phishing per ottenere i dati di accesso alla posta elettronica
Fonte	Amministrazione dell'istituto di istruzione / Germania
Periodo di riferimento	Marzo 2022
Tag	PMI, phishing, dati di accesso, spam
Stato	Risolto
Applicabilità Escape Room	Facilmente trasferibile: Il caso semplice è di facile comprensione e può essere trasferito a un modello limitato di Escape Room. Poiché si tratta di un caso standard che si verifica molto spesso, non è molto interessante per il modello.

Tipo di attacco

Phishing

Debolezza/Vulnerabilità:

Non c'è stato alcun errore da parte della collega, che ha agito correttamente e ha segnalato l'incidente. La protezione antispam e antitruffa ha permesso il passaggio della mail poiché in questo caso è stato superato il limite di difesa prestabilito.

Che cosa è successo?

- L'impiegata dell'istituto scolastico ha ricevuto un'e-mail di phishing in cui si dice che la sua password di posta elettronica è scaduta e che deve impostarne una nuova.
- Il mittente della mail era il presunto provider: Ionos (1&1)Support.

Figura 5: Nota di sicurezza

Come è stato notato?

- Grazie alla prontezza e all'informazione del dipendente, il problema è stato notato e i colleghi hanno informato in modo proattivo l'amministratore del reparto IT. I dipendenti erano consapevoli del fatto che i vari fornitori di servizi non avrebbero mai inviato e-mail con questo contenuto. Le password non scadono nell'istituto.
- Inoltre, a un esame più attento, il mittente potrebbe essere identificato come non legittimo.

Quali misure sono state adottate?

- Il collega ha inoltrato la mail all'amministratore IT.
- Il reparto IT ha quindi iniziato a prendere le consuete misure di sicurezza:
  - In primo luogo, è stata formulata una voce nel centro messaggi per avvisare tutti gli altri colleghi che in quel momento si erano verificati attacchi di phishing.
  - Parallelamente, il mittente è stato bloccato in modo che non potesse avvenire alcuna comunicazione in background (blacklist).

Qual è il risultato delle misure di difesa?

- Poiché le vittime e i reparti IT sono praticamente impotenti contro questo tipo di attacchi di phishing e non è possibile installare meccanismi di difesa sostenibili senza limitare sensibilmente l'utente, non è stato possibile intraprendere ulteriori azioni.
- Non c'è stato alcun danno, se non il tempo di lavoro investito per risolvere l'incidente.

Lezioni apprese:
Dopo aver valutato l'incidente, sono state pianificate ulteriori campagne di prevenzione e formazione dei dipendenti per aumentare la vigilanza.

Caso 5 – Codice dannoso nell'allegato di posta elettronica

Titolo	Codice dannoso nell'allegato della posta
Fonte	Università / Germania
Periodo di riferimento	Giugno 2016
Tag	PMI, posta, allegato, spam, ransomware
Stato	Risolto
Applicabilità Escape Room	Altamente trasferibile: Il caso, semplice ma istruttivo, è di facile comprensione e può essere trasferito in un interessante modello di Escape Room. Inoltre, è possibile sviluppare uno scenario per una storia istruttiva ed emozionante a partire dal caso stesso.

Eyes On attacco Locky:
Locky è un tipo di ransomware. È stato rilasciato nel 2016, mentre gli esperti di sicurezza hanno scoperto che gli autori del malware hanno consegnato questo ransomware via e-mail chiedendo il pagamento attraverso una fattura allegata a un documento Microsoft Word dannoso che esegue macro infettive. Locky Ransomware è un malware che cripta i file importanti sul computer, rendendoli inaccessibili e inutilizzabili. Li tiene "in ostaggio" e nel frattempo chiede il pagamento di un riscatto in cambio dei file crittografati.

Tipo di attacco
Attacco Locky - Ransomware Trojan.

Debolezza/Vulnerabilità:
Errore umano - Apertura di un allegato e-mail sconosciuto. Il successo dell'attacco è stato favorito dalla disattenzione della vittima e dalla variante zero-day di questo Trojan.

Che cosa è successo?
- A un membro del team (la vittima) è stata inviata una mail con un file zip che doveva contenere delle fatture.
- Questo file zip era criptato, il che rendeva impossibile la scansione da parte dei sistemi antivirus.
- La password per il file zip era contenuta nel testo dell'e-mail.

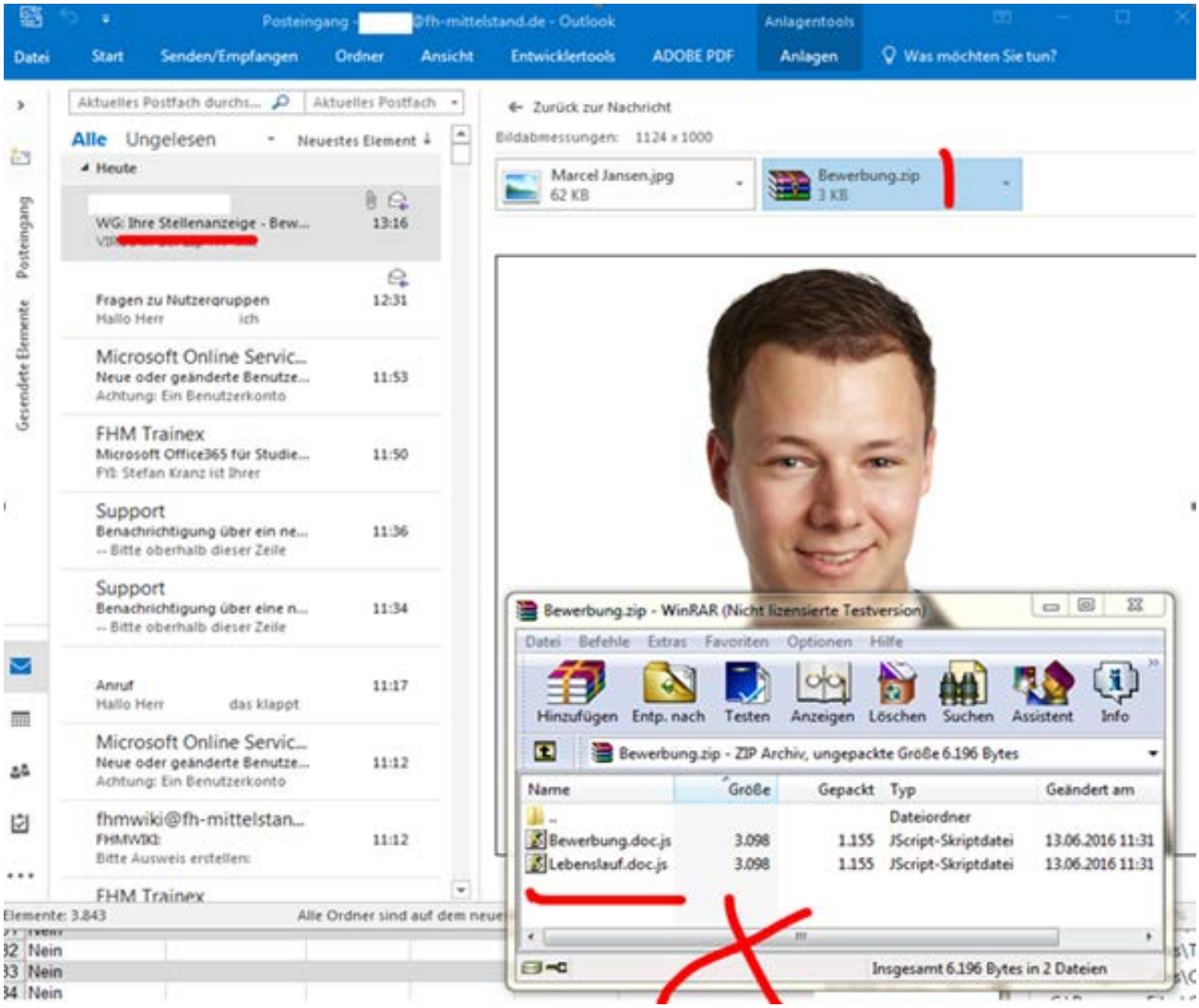


Figura 6: L'attacco pericoloso.

- La vittima ha aperto il file zip senza ulteriori verifiche, ha decompresso il file xlsm e lo ha aperto. In seguito, la vittima ha fatto la sua pausa pranzo.
- La protezione antivirus (Kaspersky) - la variante zero-day di questo Trojan - e la pausa pranzo del collega hanno fatto sì che l'applicazione avesse abbastanza tempo in background per compromettere tutti i dati.

Come è stato notato?

- Quando la vittima è tornata al suo posto di lavoro, si è chiesta perchè la schermata di sfondo fosse cambiata e ha informato il reparto IT.
- A questo punto, era passata circa un'ora da quando la vittima aveva fatto clic sul file macro-Excel allegato.
- Nel momento in cui l'amministratore si è presentato al computer della vittima per aiutare in caso di emergenza, ha immediatamente scollegato la LAN e disconnesso la WLAN.
- Purtroppo era già troppo tardi e l'attacco era stato eseguito con successo.

- L'amministratore ha trovato una situazione catastrofica: tutti i documenti erano criptati e non più utilizzabili. Oltre ai documenti locali, anche tutti i documenti accessibili sulle unità di rete erano stati crittografati.

Quali misure sono state adottate?

- Per iniziare la decrittazione, il criminale ha chiesto 500 dollari sotto forma di Bitcoin.
- Circa il 50% del personale non poteva più accedere ai documenti di lavoro presenti nell'unità di rete.
- L'amministratore ha quindi smontato il portatile in questione. Allo stesso tempo, nel Sistema di gestione clienti (CMS) è stato pubblicato un avviso sull'accaduto, in modo da ripristinare l'accessibilità telefonica.
- Il reparto IT si è immediatamente assicurato che il computer portatile causa non fosse più accessibile in rete e che nessun altro file sull'unità di rete fosse crittografato.
- Il portatile è stato completamente formattato e Windows è stato reinstallato.

Qual è il risultato delle misure di difesa tecnica / organizzativa / sociale?

- Il reparto IT, di concerto con la direzione, ha importato un backup completo del giorno precedente. Di conseguenza, tutti i processi di tutti i dipendenti delle ultime 24 ore non erano più disponibili. Per alcuni dipendenti la situazione era molto critica, ma per la maggior parte dei dipendenti il danno era limitato.
- La vittima ha ricevuto una formazione speciale per evitare di incorrere nuovamente nell'errore.
- Un giorno dopo, il fornitore di antivirus ha comunicato che anche le minacce Locky sono state rilevate e prevenute.

Caso 6 – Frode dell'amministratore delegato

Titolo	CEO-Frode
Fonte	Università / Germania
Periodo di riferimento	Aprile 2020
Tag	PMI, posta, frode, spam, truffa
Stato	Il problema esiste ancora. (Almeno tentativi simili vengono ancora rilevati, ma ora sono limitati a un numero ristretto di esempi, ad esempio le carte regalo Apple).

Applicabilità Escape Room	Facilmente trasferibile: Il caso, semplice ma istruttivo, è facile da comprendere e può essere trasferito in un modello di Escape Room interessante. Inoltre, è possibile sviluppare uno scenario per una storia istruttiva ed emozionante a partire dal caso.

Eyes On frodi agli amministratori delegati:
L'aggressore sostiene di essere il CEO di una determinata azienda e cerca di costringere la vittima a condurre azioni dannose e/o frodi a nome del vero CEO.

Che tipo di attacco è stato?

La frode CEO è una forma altamente mirata di spear-phishing in cui gli aggressori ricercano online le potenziali vittime e le loro aziende, apprendendo tutto ciò che possono dal sito web dell'organizzazione, nonché informazioni da siti di social media come LinkedIn, Facebook e Twitter. In genere, l'aggressore mira a indurre l'utente a trasferire denaro su un conto bancario di sua proprietà, a inviare informazioni riservate sulle risorse umane o a rivelare altre informazioni sensibili.

Debolezza/Vulnerabilità:

- Si tratta di una frode dell'amministratore delegato. Il mittente sostiene di appartenere alla direzione con l'intento di condurre una frode.
- La protezione antispam del provider di posta elettronica non ha funzionato o ha segnalato una "frode".
- Il dipendente non è stato addestrato a riconoscere immediatamente le richieste non legittime. Il dipendente era inoltre nuovo in azienda e aveva pochi contatti con gli altri colleghi.

Che cosa è successo?

- Un'e-mail, presumibilmente proveniente dalla direzione, arriva ai colleghi: È stato richiesto un trasferimento di denaro in un paese straniero.
- Non si tratta di una mail automatica; la persona contattata avrebbe potuto avviare il trasferimento.
- Poiché il vero indirizzo di posta dell'aggressore è difficile da riconoscere per il destinatario, l'utente non se ne è accorto.

Come è stato notato?

- Poiché il trasferimento di denaro segue regole specifiche e un meccanismo di controllo interno all'organizzazione, non è stato possibile confermare la legittimità del trasferimento. È apparso subito chiaro che si trattava di un caso di frode.
- Se l'utente avesse passato il mouse direttamente sull'indirizzo di posta, si sarebbe subito accorto che si trattava di un tentativo di frode.

Quali misure sono state adottate?

- L'attacco è stato gestito bloccando l'account di posta del mittente (l'account Gmail dell'attaccante).
- Il caso è stato segnalato alla polizia, ma non è stato identificato alcun colpevole.

Qual è il risultato delle misure di difesa?

Una protezione sostenibile entrerebbe in conflitto con l'invio di posta, va quindi rafforzata proattivamente.

Caso 7 – Backdoor nel software – Attacco spia

Titolo	Backdoor nel software - Attacco spia
Fonte	Ministero dell'Interno NRW/Düsseldorf/Germania
Periodo di riferimento	Non divulgato.
Tag	Attacco spia, backdoor
Stato	Risolto
Applicabilità Escape Room	Altamente trasferibile: L'interessante caso è di facile comprensione e può essere trasferito in un interessante modello di Escape Room. Inoltre, è possibile sviluppare uno scenario per una storia istruttiva ed emozionante a partire dal caso.

Eyes on Attacco Spia
Il furto dei risultati della ricerca, delle informazioni sullo sviluppo dei prodotti, dei dati di bilancio e dei dati dei clienti causa danni a lungo termine alle aziende interessate: i concorrenti stranieri ottengono i dati gratuitamente. Un vantaggio competitivo faticosamente conquistato può andare perduto, con un conseguente calo delle vendite dei prodotti.
I servizi segreti stranieri hanno ottime competenze informatiche e nascondono il loro accesso. Spesso la scoperta di un attacco avviene solo quando un informatore esterno avverte l'azienda dell'attacco.

Tipo di attacco
Attacco spia, backdoor

Debolezza/Vulnerabilità:
Il software di terzi non avrebbe dovuto essere utilizzato senza controllo nella rete aziendale. Al contrario, si sarebbe dovuto utilizzare un modello di sicurezza per verificare se il software potesse essere utilizzato in modo isolato.

Che cosa è successo?
- Le aziende che hanno rapporti commerciali con l'estero sono spesso obbligate a utilizzare determinati software, ad esempio per l'elaborazione degli obblighi fiscali.
- Uno speciale software backdoor è stato installato su vari computer dell'azienda della vittima collegati in rete a livello globale.
- Tramite una backdoor nascosta, un aggressore è stato in grado di accedere ai documenti nella rete della vittima.

Come è stato notato?
All'indomani dell'installazione, si viene a sapere che il software obbligatorio contiene una backdoor per i servizi segreti stranieri.

Quali misure sono state adottate?
Il sistema è stato completamente reinstallato e la backdoor è stata chiusa.

Qual è il risultato delle misure di difesa tecniche / organizzative / sociali?
Sono stati evitati ulteriori attacchi.

Caso 8 – Social engineering – Attacco spia

Titolo	Social engineering – Attacco spia
Fonte	Ministero dell'Interno NRW/Düsseldorf/Germania
Periodo di riferimento	Non divulgato.
Tag	Attacco spia, Social Engineering
Stato	Risolto
Applicabilità Escape Room	Altamente trasferibile: Il caso interessante è di facile comprensione e può essere trasferito in un modello interessante di Escape room. Inoltre, è possibile sviluppare uno scenario per una storia istruttiva ed emozionante a partire dal caso stesso.

Tipo di attacco
Attacco di spie

Debolezza/Vulnerabilità:
Gli aggressori sanno abilmente come creare nella vittima la paura di perdere una buona offerta. Inoltre, il contatto telefonico riduce la diffidenza nei confronti dell'aggressore. Tuttavia, il documento dannoso non avrebbe dovuto essere aperto nella rete aziendale. Ancora una volta viene sfruttata la "debolezza umana".

Che cosa è successo?
- In molti settori dell'alta tecnologia, è frequente che gli individui vengano contattati da reclutatori con offerte di cambio di lavoro.
- Quando un dipendente di una nota azienda riceve una chiamata sul cellulare da parte di un cacciatore di teste, non sembra una cosa fuori dal comune. Dopo una breve conversazione, il presunto agente annuncia che inoltrerà una vantaggiosa offerta di lavoro. Poco dopo, il documento arriva nell'account WhatsApp del dipendente. Quando cerca di aprirlo sul cellulare, il processo si interrompe con un messaggio di errore.
- Il giorno successivo, il cacciatore di teste contatta nuovamente il dipendente e gli promette un potenziale di guadagno eccezionale con condizioni di lavoro interessanti. Tuttavia, è necessario fornire immediatamente un feedback sull'interesse per l'offerta fatta. Senza ulteriori indugi, il dipendente trasferisce il documento ricevuto alla presentazione al suo account di posta elettronica aziendale. Dopo una breve conferma di utilizzo di un modello di formato speciale, può aprire il file sul suo computer aziendale. Poiché l'offerta

non soddisfa le sue aspettative, cancella il lavoro con il cacciatore di teste. Dopodiché, il processo viene dimenticato.
- In seguito si è scoperto che aprendo il documento è stato stabilito un accesso remoto al PC aziendale del dipendente. Questo accesso ha permesso agli aggressori di diffondersi ulteriormente nella rete aziendale e di far trapelare dati sensibili. Il furto di dati è stato notato solo quando gli aggressori erano ormai scomparsi da tempo.

Come è stato notato?
Non ci sono ulteriori informazioni, perché il caso non è stato divulgato dal Ministero dell'Interno NRW.

Quali misure sono state adottate?
Non ci sono ulteriori informazioni, perché il caso non è stato divulgato dal Ministero dell'Interno NRW.

Qual è il risultato delle misure di difesa?
Non ci sono ulteriori informazioni, perché il caso non è stato divulgato dal Ministero dell'Interno NRW.

Caso 9 – Mail di phishing

Titolo	Mail di phishing
Fonte	Società di notizie IT, Germania
Periodo di riferimento	Maggio 2019
Tag	Azienda, phishing, attacco via e-mail, ransomware
Stato	Risolto entro alcune settimane dal verificarsi del problema, con la creazione di una nuova rete e la sostituzione di tutti i computer collegati alla rete durante l'attacco.
Applicabilità Escape Room	Altamente trasferibile: Emotet e trojan sono comunemente conosciuti, così come il phishing.

Eyes on phishing
Abbiamo già descritto gli attacchi di phishing, ma è importante notare che gli attacchi di phishing si sono adattati nel corso degli anni e stanno diventando sempre più "migliori" e sofisticati. È quindi importante tenersi aggiornati sui metodi di phishing più recenti.

Tipo di attacco
Attacco di phishing

Debolezza/Vulnerabilità:
Il dipendente ha attivato le macro per il file infetto.

Che cosa è successo?
- Un dipendente ha aperto un messaggio di posta elettronica proveniente da un mittente spoofato che si spacciava per un partner commerciale. L'e-mail conteneva un documento Word infetto.
- Quando il dipendente ha aperto questo file, è apparso un messaggio di errore che richiedeva al dipendente di "abilitare" la modifica.
- Il dipendente ha cliccato su questo messaggio ed Emotet ha infettato il suo sistema e ha iniziato a diffondersi nella rete.

Come è stato notato?
Sono state rilevate diverse infezioni e sono stati trovati diversi computer infetti in tutta la rete.

Quali misure sono state adottate?
- Sono state stabilite le connessioni tra i vari computer e l'esterno.
- Il virus è stato rimosso con Avira e Windows Defender.
- In seguito, gli amministratori hanno cercato di impedire al malware di comunicare con l'infrastruttura Emotet. Poiché non ha funzionato come previsto, l'intera rete è stata scollegata da Internet.
- Sono stati contattati fornitori di servizi esterni e diverse società di informatica forense.

Qual è il risultato delle misure di difesa?
- L'intera intranet è stata ripristinata e tutti i computer collegati alla intranet durante l'attacco sono stati sostituiti.
- Il concetto di sicurezza è stato rivisto per evitare questo caso in futuro.

Caso 10 – Mail di phishing del ricattatore

Titolo	Mail di phishing del ricattatore
Fonte	Grossista di materiale elettrico (Germania)
Periodo di riferimento	Febbraio 2020
Tag	Azienda, phishing, attacco via e-mail, PMI, ransomware
Stato	Risolto entro tre settimane dal verificarsi del problema pagando il riscatto.
Applicabilità Escape Room	Altamente trasferibile: I backup mancanti sono un grosso problema e la perdita di dati senza un backup funzionante è catastrofica.

Eyes on backup
Un backup è una copia dei dati che viene realizzata e conservata separatamente dai dati originali. Questa copia può essere utilizzata per ripristinare i dati originali in caso di perdita o danneggiamento. È consigliabile creare e testare regolarmente i backup all'interno di un'azienda.

Tipo di attacco
Attacco di phishing

Debolezza/Vulnerabilità:
L'e-mail infetta è stata aperta inavvertitamente da un dipendente. Il ransomware ha crittografato tutti i file. Un'apertura negligente di e-mail e allegati sospetti ha portato alla riuscita dell'attacco. Inoltre, l'azienda non aveva una strategia di backup regolare. La mancanza di controlli di backup li ha costretti a pagare il riscatto.

Che cosa è successo?
- Un dipendente ha aperto un allegato di posta elettronica infetto. Tutti gli annunci erano bianchi e mostravano un indirizzo e-mail. Il ceppo di malware Emoted ha infettato tutti i computer e ha quindi crittografato tutti i file a portata di mano.
- Un fornitore di servizi esterno, incaricato di creare i backup, non li aveva ancora creati. Non era disponibile alcun backup recente e gli unici disponibili erano troppo vecchi per essere utilizzati.
- Nessuno supervisionava i backup e aveva controllato la data degli ultimi backup. Anche la comunicazione con il fornitore esterno di servizi non era regolare.

Informazioni aggiuntive: Le macro sono spesso utilizzate nelle applicazioni di Office come Word, Excel e PowerPoint. Queste macro vengono salvate come parte del file del documento e sono scritte in un linguaggio di programmazione chiamato VBA (Visual Basic for Applications). Le macro possono essere utilizzate per infettare un sistema con malware.

Come è stato notato?

I file sono stati crittografati rapidamente e il sistema non era utilizzabile.

Quali misure sono state adottate?

- L'azienda ha contattato la polizia e il ricattatore.
- Il ricattatore ha chiesto 21 Bitcoin, corrispondenti a 120.000 euro. Senza un backup funzionante, la loro stessa esistenza era a rischio. Pertanto, il riscatto è stato pagato e tutti i sistemi sono stati decriptati.
- Comunicazione per posta e assenza di fatturazione digitale per tre settimane, con conseguenti ingenti perdite finanziarie.

Informazioni aggiuntive: Non tutte le aziende che pagano il riscatto ottengono che i loro file vengano decriptati. Anche se i file vengono recuperati, è necessario esaminare tutti i file per verificare la presenza di malware nascosto.

Qual è il risultato delle misure di difesa?

- Il sistema di posta elettronica è passato a una soluzione cloud di Microsoft.
- I backup esterni vengono ora creati settimanalmente.
- Sono stati attivati regolari piani di backup e di sicurezza.
- Formazione sulla sicurezza informatica

Caso 11 – Mail di phishing con malware

Titolo	Mail di phishing con malware
Fonte	Società di sicurezza delle macchine (Germania)
Periodo di riferimento	Maggio 2020
Tag	azienda, phishing, attacco via e-mail, ransomware
Stato	Risolto entro due settimane dalla chiusura di Intranet.
Applicabilità Escape Room	Altamente trasferibile: Le e-mail sono pericolose, i suggerimenti delle autorità pubbliche devono essere presi sul serio e verificati

Eyes On malware
Il malware, abbreviazione di software maligno, è un software progettato per danneggiare o sfruttare un sistema informatico o una rete. Esistono diversi tipi di malware, tra cui virus, worm, cavalli di Troia, ransomware e spyware. Spesso è allegato e nascosto in altri software o link.

Tipo di attacco
Phishing

Debolezza/Vulnerabilità:
Apertura negligente di un allegato e-mail infetto. I dipendenti non sono stati formati adeguatamente per essere in grado di rilevare un'e-mail sospetta.

Che cosa è successo?
È stata aperta un'e-mail con malware.

Come è stato notato?
- L'azienda è stata informata da un'autorità pubblica (Landeskriminalamt) di un imminente attacco informatico, tramite e-mail infette.
- L'azienda ha verificato la chiamata e ha deciso di disconnettere la rete sette minuti dopo la chiamata.

Quali misure sono state adottate?
- Disconnessione della rete
- Esame e disinfezione di tutti i sistemi della rete. Dopo la disconnessione, il malware è stato identificato. La produzione si è fermata.
- Ogni computer doveva essere ripristinato singolarmente.
- La comunicazione via e-mail è avvenuta grazie ad un server sostitutivo.

Informazioni aggiuntive: il ripristino individuale di ogni computer è molto costoso in termini di tempo e di costi per l'azienda. L'attacco avrebbe potuto essere evitato con una formazione adeguata.

Qual è il risultato delle misure di difesa tecniche / organizzative / sociali?
Due settimane dopo, il sistema informatico e la produzione erano di nuovo operativi.

Caso 12 – Ransomware e phishing

Titolo	Ransomware e phishing
Fonte	Fornitore di servizi IT
Periodo di riferimento	Ottobre 2021
Tag	azienda, PMI, ransomware
Stato	In corso, il 95% dei sistemi è stato ripristinato.
Applicabilità Escape Room	Altamente trasferibile: Il recupero dopo un attacco riuscito deve essere addestrato per essere veloce ed efficiente.

Eyes On DeepBlueMagic
DeepBlueMagic sembra provenire dalla Cina. Come diversi ceppi di ransomware in passato, cripta i file utilizzando strumenti di crittografia comuni come Bitlocker e BestCrypt, di cui gli utenti spesso si fidano e che utilizzano per la crittografia stessa.

Tipo di attacco
Il malware "DeepBlueMagic" è stato installato tramite mail di phishing.

Debolezza/Vulnerabilità:
Apertura negligente di un allegato e-mail infetto. I dipendenti non sono stati formati adeguatamente da rilevare un'e-mail sospetta.

Che cosa è successo?
- I provider delle autorità pubbliche sono stati attaccati. È stato aperto un allegato e-mail infetto contenente malware.
- Non sono stati rubati dati personali.

Come è stato notato?
Gli utenti hanno ricevuto e-mail dai criminali informatici in cui si diceva che i loro file erano criptati e non utilizzabili.

Quali misure sono state adottate?
- L'ufficio amministrativo regionale ha dovuto chiudere.

- Tutti i sistemi sono stati disattivati.
- Oltre ai sistemi principali, è stato necessario analizzare 4.000 dispositivi finali alla ricerca di malware.
- I backup sono stati ripristinati, ma il ripristino è ancora in corso.
- Non è stato pagato alcun riscatto.

Informazioni aggiuntive: Questo esempio dimostra quanto sia importante un sistema di backup funzionante. Anche dopo l'attacco sono riusciti a ripristinare i dati senza pagare il riscatto. Ricordate: niente backup - niente pietà.

Qual è il risultato delle misure di difesa?

Alla fine del 2021, il 95% dei dati era stato ripristinato.

Caso 13 – Malware

Titolo	Malware
Fonte	Start-up di investimento (Germania)
Periodo di riferimento	Ottobre 2021
Tag	azienda, PMI, ransomware, Social Engineering
Stato	Risolto dopo pochi giorni chiudendo la vulnerabilità sfruttata.
Applicabilità Escape Room	Trasferibile con difficoltà: Lo sfruttamento delle vulnerabilità richiede un certo livello di conoscenza o deve essere molto facile da individuare. Tuttavia, richiedono una comprensione più approfondita delle tecnologie informatiche.

Eyes On 'Social Engineering'

Social Engineering è l'uso della manipolazione psicologica per influenzare individui o gruppi a divulgare informazioni sensibili o eseguire azioni che potrebbero essere dannose per loro o per l'organizzazione. Può includere tattiche come il phishing, il vishing (phishing vocale) e la manipolazione telefonica. L'obiettivo è sempre lo stesso: ingannare le persone per indurle a cedere informazioni riservate o accesso a sistemi o reti.

Tipo di attacco
Attacco ransomware supportato da telefonate di social engineering.

Debolezze/Vulnerabilità
I dati rubati sono stati utilizzati per supportare e dare credibilità alle telefonate di social engineering.

Che cosa è successo?
- Attacchi di phishing supportati da telefonate di social engineering verso i clienti.
- La vulnerabilità del sistema informatico non è stata individuata in tempo.
- La vulnerabilità del sistema è stata sfruttata per far trapelare i dati dei clienti.

Come è stato notato?
Durante una scansione del sistema, la falla di sicurezza/attacco è stata localizzata rapidamente.

Quali misure sono state adottate?
- I clienti e le autorità sono stati informati.
- La vulnerabilità è stata risolta.

Informazioni aggiuntive: Se un utente deve cambiare la password, è consigliabile che il dipartimento IT competente pubblichi i requisiti relativi alle password “forti”.

Qual è il risultato delle misure di difesa?
Dopo la risoluzione della vulnerabilità, i clienti sono stati avvisati e invitati a modificare le loro password.

Caso 14 – Malware in azienda

Titolo	Malware in azienda
Fonte	Produttore di macchinari industriali (Germania)
Periodo di riferimento	Luglio 2021
Tag	Azienda
Stato	Risolto dopo qualche mese.
Applicabilità Escape Room	Trasferibile con difficoltà: Il caso era molto elaborato e non era assolutamente colpa dell'azienda - lezione da imparare: non importa quanto sia buona la vostra sicurezza, può sempre esserci un attacco.

Eyes On mail spoof
Un'email spoof è un'email in cui l'indirizzo email del mittente e altre parti dell'intestazione dell'email sono state alterate per far sembrare che l'email provenga da una fonte diversa. Questa tecnica è spesso utilizzata nelle truffe di phishing e in altre forme di frode, in quanto può far apparire l'e-mail più legittima al destinatario.

Tipo di attacco
Attacco elaborato e pianificato da tempo, che utilizza un fornitore di servizi estero per entrare in azienda tramite una mail di phishing e un sito web falso.

Debolezze/Vulnerabilità
Il fornitore di servizi è stato usato come punto debole, sebbene la sicurezza informatica e il personale dell'azienda fossero ben preparati.

Che cosa è successo?
Gli hacker hanno inviato una mail fasulla a un fornitore di servizi estero. La mail era collegata a un sito web perfettamente contraffatto, in modo che il fornitore di servizi non potesse riconoscere la frode.

Come è stato notato?
Il sistema aziendale è andato fuori uso automaticamente e tutti i file sono stati crittografati.

Quali misure sono state adottate?

- Tutti i sistemi sono stati spenti.
- Tutti i processi aziendali sono stati interrotti.
- Tentativo di ricatto con il gruppo Conti.
- Un fornitore esterno di sicurezza informatica è stato incaricato di ripristinare i sistemi.

Informazioni aggiuntive: Anche se un sistema di sicurezza funziona bene e il personale è adeguatamente addestrato, è sempre possibile subire una violazione. Purtroppo non è possibile tutelarsi dagli attacchi al 100%.

Qual è il risultato delle misure di difesa?

- È stata fondata una task force.
- Le autorità pubbliche sono state informate.
- Sono state definite le priorità delle diverse aree di business.
- L'infrastruttura è stata ricostruita, sono stati coinvolti consulenti e supporto IT esterni.
- I backup sono stati ripristinati secondo tre categorie: rosso (ancora infetto), arancione (in quarantena) e verde (dati puliti).

5.3 Sicurezza informatica Casi dal Portogallo

Caso 1 – Denial of Service nei servizi di comunicazione

Titolo	Denial of Service nei servizi di comunicazione
Fonte	Wikipedia[23], Diário de Notícias[24]
Periodo di riferimento	Febbraio 2021
Tag	Azienda, telecomunicazioni
Stato	Risolto
Applicabilità Escape Room	Facilmente trasferibile: Il caso potrebbe essere trasferito al modello di Escape room. Tuttavia, l'azienda non ha rivelato informazioni sufficienti a fornire uno scenario per il gioco.

Tipo di attacco

Si sospetta che un gruppo altamente sofisticato di hacker abbia condotto l'attacco sfruttando alcune falle di sicurezza in un software non aggiornato, ma l'exploit utilizzato non è stato rivelato. L'attacco prevedeva che l'azienda non potesse fornire i propri servizi di comunicazione.

Debolezze/Vulnerabilità:

I punti deboli derivavano dal mancato aggiornamento di tutti i software che gestivano i servizi di comunicazione. Non è chiaro se ci sia stata anche una collaborazione interna.

Che cosa è successo?

Gli hacker hanno sfruttato la vulnerabilità del software per accedere ai server e ai sistemi di comunicazione e causare guasti nella comunicazione.

Come è stato notato?

- Mancanza di dati mobili su rete 3G e 4G.
- Mancanza di servizi di SMS, TV e Internet fisso.
- Mancanza di servizio vocale.
- Il 112 (numero dei servizi di emergenza) non raggiungibile.
- SIBS [proprietaria del marchio Multibanco] è un cliente Vodafone. La loro rete ATM

23 https://pt.wikipedia.org/wiki/Ciberataque_%C3%A0_Vodafone_Portugal
24 https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

era supportata dalla rete Vodafone. Alcuni sportelli automatici, avendo una rete di interconnessione con la rete dati mobile, non erano disponibili fino a mezzanotte circa:
- I negozi non potevano vendere i loro prodotti online perché i collegamenti con il principale operatore bancario non funzionavano.
- I clienti non hanno potuto utilizzare i bancomat.
- I clienti non potevano pagare nei negozi con le carte.

Quali misure sono state adottate?

I servizi di emergenza e sanitari sono stati dirottati su altre società di comunicazione. L'azienda ha dovuto fermare tutti i sistemi dovendo tornare a sistemi di comunicazione più vecchi. Poi, gradualmente, ha dovuto controllare e riavviare tutti i sistemi interessati. Ci sono volute circa due settimane.

Qual è il risultato delle misure di difesa?

Grazie alle nuove misure di sicurezza implementate, i servizi non sono più stati attaccati dopo l'incidente.

Errori e reazioni:

L'interruzione di Vodafone è avvenuta per opera di hacker che hanno sfruttato una vulnerabilità del software. Le persone sono rimaste molto turbate e alcune hanno iniziato a farsi prendere dal panico, perché non potevano raggiungere altre persone o contatti di emergenza come il 112, alcune aziende hanno perso molto denaro e le persone temevano che gli hacker avessero accesso a informazioni private. Tuttavia, l'amministratore delegato di Vodafone ha garantito che non c'è stato alcun accesso a informazioni private. L'azienda ha poi rafforzato le misure di sicurezza.

Caso 2 – Phishing nei clienti dei negozi al dettaglio

Titolo	Phishing nei clienti dei negozi al dettaglio
Fonte	Diário de Notícias[25]
Periodo di riferimento	Novembre 2019
Tag	Azienda
Stato	Risolto
Applicabilità Escape Room	Facilmente trasferibile

Tipo di attacco
Attacco di phishing ai clienti di un grande negozio al dettaglio.

Debolezze/Vulnerabilità:
L'approccio di social engineering è stato molto ben fatto e ha approfittato di clienti ignari.

Che cosa è successo?
Le persone hanno ricevuto falsi messaggi da persone che si spacciavano per dipendenti del negozio al dettaglio (Continente) e chiedevano informazioni personali. Alcune persone hanno dato credito ai messaggi fornendo i loro dati personali agli hacker.

Come è stato notato?
Le persone hanno iniziato a vedere gli articoli acquistati con la carta del negozio al dettaglio.

Quali misure sono state adottate?
I clienti sono stati informati e avvertiti dell'attacco. I clienti colpiti hanno ricevuto nuove carte.

Qual è il risultato delle misure di difesa?
La campagna informativa ha evitato che un gran numero di clienti venisse colpito.

Errori e reazioni:
I clienti del negozio al dettaglio sono stati vittime di phishing e non hanno controllato la veridicità delle informazioni contenute nei messaggi e-mail.

25 https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

Caso 3 – Dati rubati a enti pubblici.

Titolo	Dati rubati a enti pubblici
Fonte	NOTIZIE RTP[26]
Periodo di riferimento	Tra Maggio e Dicembre 2017
Tag	Aziende, istituzioni pubbliche, privati
Stato	Risolto
Applicabilità Escape Room	Facilmente trasferibile: • È un caso rilevante da approfondire, soprattutto in considerazione del suo ampio impatto e dell'alto profilo delle vittime (che avrebbe potuto portare a gravi conseguenze e alla condivisione di informazioni riservate). • Abbiamo informazioni sugli aspetti tecnici dell'attacco (le password sono state rubate attraverso registrazioni su canali di social media e i dati sono stati pubblicati su due liste online - "Exploit.in" e "Anti Public" - che circolano nel dark web. • Possiamo dividere la narrazione in diversi momenti: da quando è stato dato il primo segnale d'allarme e sono stati condivisi i primi dati (intorno al 2016), a quando sono stati trovati gli elenchi finali e l'attacco è stato reso pubblico.

Tipo di attacco

Gli hacker hanno sfruttato le vulnerabilità del software nei server delle istituzioni pubbliche che non erano stati mantenuti in modo adeguato dal punto di vista della sicurezza informatica.

Debolezze/Vulnerabilità

I principali errori che si possono evidenziare in questa situazione sono diversi:

- Gli indirizzi e-mail professionali e ufficiali sono stati utilizzati dagli individui per registrarsi sui canali dei social media e su altre piattaforme,
- Dopo l'evento non sono state adottate misure per proteggere gli account rivelati (ad esempio, modificando le password esposte).

26 https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761

Che cosa è successo?

- Secondo la fonte, un documento di 20.416 pagine (con un totale di quasi 32,5 milioni di password) circolava su Internet, rivelando dati appartenenti a dipendenti e rappresentanti di quasi tutti i settori della pubblica amministrazione, come ministeri, forze armate, forze di pubblica sicurezza, autorità fiscali e commissione elettorale nazionale.
- Le vittime sono state molteplici e diverse: enti pubblici, grandi aziende, enti governativi, dipendenti pubblici e squadre di calcio.
- Inoltre, sono state rivelate anche le password e le e-mail di persone che lavorano in luoghi pubblici e privati, come banche, ospedali e media. Secondo le informazioni rivelate all'epoca, i dati personali degli utenti erano già stati rubati anni prima della pubblicazione, e gli hacker li avevano raccolti attraverso attacchi agli account dei social media, come Facebook, LinkedIn, Twitter, e alle piattaforme di archiviazione, come Dropbox. Questo attacco è stato definito il più grande attacco informatico e il più grande furto di informazioni mai registrato in Portogallo.

Come è stato notato?

Il 20 Dicembre 2017, una testata giornalistica portoghese ha pubblicato un articolo in cui si rivelava che migliaia di e-mail e password erano state rubate da un gruppo di hacker.

Quali misure sono state adottate?

- La polizia giudiziaria ha prontamente avviato un'indagine sull'attacco. Tuttavia, un rappresentante delle forze di sicurezza ha ammesso che le informazioni non erano recenti e, in realtà, erano note da tempo (dal 2016).
- Dopo l'evento non sono state adottate misure per proteggere gli account rivelati (ad esempio, modificando le password esposte).

Qual è il risultato delle misure di difesa?

In questo senso, e dato che molte delle password rivelate erano ancora attive circa un anno dopo la violazione dei dati[27], si può concludere che c'è ancora una mancanza di conoscenza della sicurezza online in diverse istituzioni pubbliche e private portoghesi.

27 https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal

Caso 4 – Negazione del servizio in una PMI

Titolo	Negazione del servizio in una PMI
Fonte	Fonte interna
Periodo di riferimento	Tra Gennaio e Febbraio 2022
Tag	PMI
Stato	Risolto
Applicabilità Escape Room	Facilmente trasferibile: Il caso potrebbe essere trasferito al modello Escape room perché mostra un problema semplice che può riguardare la maggior parte delle PMI. Gli aspetti tecnici del caso sono facilmente accessibili.

Tipo di attacco
Negazione del servizio in una PMI

Debolezze/Vulnerabilità
La causa identificata è stata un attacco alle password che ha permesso di appropriarsi indebitamente di un account di posta elettronica del personale che non utilizzava uno sistema di generazione delle password appropriato.

Che cosa è successo?
- Un attacco con password che si appropria di un account. Gli hacker utilizzano poi quell'account per generare messaggi di posta fasulli.
- Alcuni account e il server di posta elettronica venivano utilizzati per spammare alcuni indirizzi e causare Denial of Service. Il dominio della PMI è stato anche inserito nella lista nera di alcuni servizi.

Come è stato notato?
L'amministratore di sistema ha iniziato a ricevere centinaia di avvisi relativi a messaggi non inviati o inviati a indirizzi sbagliati. Poi ha contattato il provider di servizi Internet, avvertendolo della situazione.

Quali misure sono state adottate?
Il provider Internet che supporta la PMI ha chiuso tutti gli accessi ai siti web e agli ambienti online, tranne quelli utilizzati per l'amministrazione. Le password sono state cambiate e i file sono stati ripuliti. Sono stati adottati migliori sistemi di generazione di password.

Qual è il risultato delle misure di difesa?
Non si sono ripetute le irruzioni, anche se gli attacchi sono ancora frequenti.

Caso 5 – Iniezione di codice nei siti web

Titolo	Iniezione di codice nei siti web
Fonte	Fonte interna
Periodo di riferimento	Tra Ottobre 2021 e Marzo 2022
Tag	PMI
Stato	Risolto
Applicabilità Escape Room	Facilmente trasferibile: Il caso potrebbe essere trasferito al modello Escape room perché mostra un problema semplice che può riguardare la maggior parte delle PMI. Gli aspetti tecnici del caso sono facilmente accessibili.

Tipo di attacco
Sfruttamento software di alcuni plugin di WordPress. Il codice è stato iniettato in questi file.

Debolezze/Vulnerabilità
Il personale della PMI non utilizzava misure adeguate a proteggere i siti web.

Che cosa è successo?
- Installazione trojan.
- Eseguire il software (trojan).
- Generare voci di registro per riempire lo spazio su disco.

Come è stato notato?
L'ISP esegue controlli di sicurezza regolari sui server che hanno rilevato il virus iniettato.

Quali misure (tecniche) sono state adottate?
I file sono stati puliti e tutti i plugin sono stati aggiornati.

Qual è il risultato delle misure di difesa tecniche / organizzative / sociali?
Non si sono ripetute le irruzioni, anche se gli attacchi sono ancora frequenti.

Caso 6 – Dati rubati da una squadra di calcio

Titolo	Dati rubati da una squadra di calcio
Fonte	Tutti i media in Portogallo
Periodo di riferimento	Tra il 2018 e il 2019
Tag	Azienda
Stato	In corso
Applicabilità Escape Room	Trasferibile con difficoltà: Il caso potrebbe non essere trasferito al modello Escape Room perché gli aspetti tecnici del caso non sono facilmente accessibili.

Tipo di attacco
Non è chiaro se il criminale informatico abbia avuto accesso tramite phishing o attacco con password.

Debolezze/Vulnerabilità:
Mancanza di misure di sicurezza efficaci nei sistemi utilizzati da persone con scarse competenze digitali.

Che cosa è successo?
- Gli hacker hanno avuto accesso alle e-mail del consiglio di amministrazione di un importante club di calcio Portoghese.
- Un archivio con diversi terabyte di messaggi di posta elettronica è stato messo a disposizione di un canale di notizie che li ha resi pubblici. Alcuni dei messaggi indicavano la corruzione e la concussione di diversi agenti sportivi da parte dei funzionari del club.

Come è stato notato?
Un canale di informazione pubblico ha ricevuto il database con i messaggi e-mail e li ha resi pubblici.

Quali misure sono state adottate?
L'hacker responsabile è stato identificato e arrestato. Il caso è attualmente sotto processo. Il club interessato ha scelto una nuova soluzione per gestire la messaggistica.

Qual è il risultato delle misure di difesa?
Il club non dipende più dai tecnici interni di sicurezza informatica, che evidentemente non erano all'altezza della sfida.

6 Conclusioni

La maggior parte dei casi illustrati in questo compendio afferma che il grado di protezione delle PMI non è correlato all'innovazione e al progresso digitalizzato in continua espansione. Persistono debolezze e vulnerabilità tra i membri del personale che spesso utilizzano i dispositivi finali senza la dovuta cura e attenzione alla cybersecurity. La mancanza di competenze e conoscenze sulle minacce informatiche, così come l'entità dei possibili danni all'azienda o alla propria persona, esistono ancora.
Gli esempi raccolti in tre Paesi europei hanno rivelato che i problemi e le sfide affrontate dalle PMI europee sono comparabili. Questa somiglianza permette di elaborare soluzioni collaborative per migliorare lo stato esistente. In generale, è importante evidenziare i rischi e le ripercussioni individuali di comportamenti inalterati, incauti e incuranti, e fornire indicazioni su come agire e reagire correttamente. Dato che le piccole e medie imprese contribuiscono alla stabilità economica di tutte le nazioni europee, diventa particolarmente cruciale sensibilizzare i dipendenti, contribuendo così alla resilienza e alla sicurezza digitale dell'Europa.
La natura e il tipo di vulnerabilità sono coerenti e comparabili tra le PMI: phishing, social engineering, ransomware e password non sicure. Una parte significativa di questi attacchi può essere attribuita a errori umani. Molte aziende hanno applicato approcci simili per contrastare gli attacchi e correggere la situazione attraverso l'implementazione di misure di sicurezza tecniche e organizzative.
Tuttavia, non tutti i leader delle PMI hanno interiorizzato le lezioni apprese. In diverse aziende, i leader hanno istituito sistemi preventivi contro i cyberattacchi e le minacce, mentre solo poche hanno scelto la formazione del personale come misura di sicurezza successiva. Questa opzione sembra essere meno prioritaria e meno comunemente perseguita, finora.

Le reazioni e le risposte agli attacchi informatici nelle PMI in mostra rivelano una carenza nella comprensione e nel riconoscimento dell'importanza e del valore dell'istruzione e della formazione in questo settore. Questi risultati sottolineano ancora una volta la necessità impellente di creare e fornire opportunità e programmi educativi volti a mitigare le lacune di competenza del personale non tecnico. Dotare le aziende e le organizzazioni di conoscenze e competenze essenziali è fondamentale per garantire operazioni efficaci e sicure nei processi aziendali.
Questo compendio è stato pubblicato per supportare le PMI nell'affrontare gli attacchi alla sicurezza informatica. Lo stesso progetto EyesOnCS vuole contribuire alla formazione in materia di sicurezza informatica del personale delle PMI europee e degli studenti delle scuole professionali.

7 Bibliografia

- Abt, C., Serious Games (1987): University Press of America.
- Agrawal, S.; Simon, A.; Bech, S.; Bæntsen, K.; Forchhammer, S. (2020): Defining immersion. Literature review and implications for research on audiovisual experiences. J. Audio Eng. Soc., 68, 404–417.
- ACN Italy: National Cybersecurity Strategy 2022 – 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, seen 29.7.22.
- Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html , seen 28.7.22.
- Cyber security intelligence: National Cyber Security Centre Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html , seen 29.7.22.
- ENISA (2022): Consolidated Annual Activity Report 2021, Attiki, 2022.
- ENISA (2021): Cybersecurity for SMES- Challenges and Recommendations, European Union Agency for Cybersecurity (ENISA), Attiki, 2021.
- European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework , seen 29.7.22.
- EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 32019R0881 - EN - EUR-Lex , seen 28.7.22.
- EyesOnCS Projektteam (2023): Cyber Alert Scenario_0x_nn, Preliminary report of the project team, to be published, FHM Düren, Düren, 2023
- Guckian,. J., Sridhar, A. & Meggitt, S. J. (2020): Exploring the perspectives od dermatology undergraduades with an escape room game. Clinical and Experimental Dermatology, 45 (2), 153-158. https://doi.org/10.1111/ced.14039

- Juzeleniene, S., Mikelioniene, J., Escudeiro, P., Vaz de Carvalho, C. (2014): GABALL project. serious games-based language learning. Procedia-Soc. Behav. Sci. 136, 350–354.

- Mac Gregor, M. (2018). Campus Clue: Habituating Students to the Information Search Process via Gaming. Pennsylvania Libraries: Research & Practice, 6 (2), 86-92. https://doi.org/10.5195/palrap.2018.172

- Martina, Richard & Göksen, Sultan. (2020). Developing Educational Escape Rooms for Experiential Entrepreneurship Education. Entrepreneurship Education and Pedagogy. https://www.researchgate.net/publication/346548119_Developing_Educational_Escape_Rooms_for_Experiential_Entrepreneurship_Education , seen 10.1.23.

- Michael, D.R., Chen, S.L. (2006): Serious Games. Games That Educate, Train, and Inform. Thomson Course Technology PTR, Oshawa.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/ , seen 28.7.22.

- N.N.: About ENISA - The European Union Agency for Cybersecurity, https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity, seen 28.7.22.

- N.N.: https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727, seen 28.7.22.

- N.N.: https://www.dn.pt/sociedade/servicos-de-voz-movel-da-vodafone-registam-recuperacao-progressiva-14568590.html , seen 28.7.22.

- N.N.: https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html, seen 28.7.22.

- N.N.: https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761, seen 28.7.22.

- N.N.: https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal/, seen 28.7.22.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/, seen 28.7.22.

- N.N.: Deutschland sicher im Netz, https://www.sicher-im-netz.de, seen 28.7.22.

- Oblinger, D. (2006): Simulations, games, and learning. ELI White Paper, vol. 1, no. 1.http://net.educause.edu/ir/library/pdf/ELI3004.pdf.

- Prensky, M.(2003): Digital Game-Based Learning. Comput. Entertain. (CIE) 1(1), 21 .

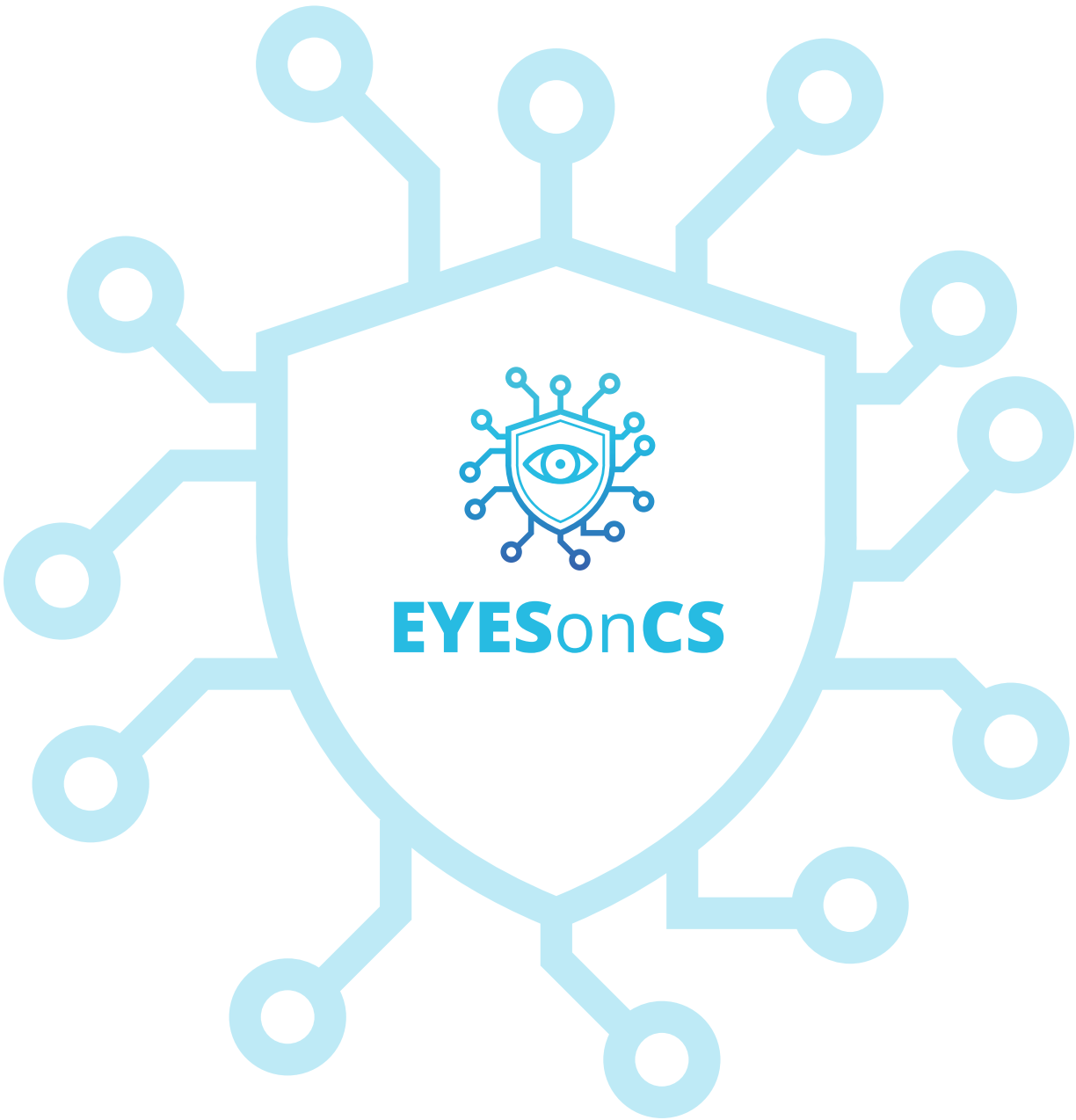
- Streim, A., Mann, S. (2021): Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, bitkom, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr , seen 2.3.23

- Tercanli, H., Martina, R., Ferreira Dias, M., Reuter, J., Amorim, M., Madaleno, M., Magueta, D., Vieira, E., Veloso C., Figueiredo, C., Vitòria, A., Wakkee, I., Gomes, I., Meireles, G., Daubariene, A., Daunoriene, A., Mortensen, A., Zinovyeva, A., Rivera-Trigueros, I., Lòpez-Alcarria, A., Rodrigìguez-Dìaz, P., Olvera-Lobo, M.D., Ruiz-Padillo, D.P., And Guitièrrez-Pèrez, J. (2021), Educational escape rooms in practice: Research, experiences and recommendations. UA Editoria. https://doi .org/10.34624/rpxk-hc61

- Zyda, M. (2005): From visual simulation to virtual reality to games. Computer 38(9), 25–32.

Note

Note



Restate sintonizzati!
Per saperne di più
sul progetto seguiteci qui:

www.eyesoncs.eu

Cofinanziato
dall'Unione europea