Università di Scienze
Applicate Zurigo

School of
Management and Law

Rischi informatici e PMI svizzere

Un'indagine sugli atteggiamenti dei dipendenti e sulle vulnerabilità comportamentali

Carlo Pugnetti, Istituto Risk & Insurance della ZHAW
Carlos Casián, Allianz Suisse

In cooperazione con:

Allianz

Editore
ZHAW School of Management and Law
St.-Georgen-Platz 2
Casella postale
8401 Winterthur
Svizzera

Istituto Risk & Insurance (IRI)
www.zhaw.ch/en/sml/institutes-centres/iri/

Autore/Contatto
Dr. Carlo Pugnetti
carlo.pugnetti@zhaw.ch

Gennaio 2021

Editoriale

L’evoluzione e la diffusione della tecnologia dischiudono modi nuovi ed entusiasmanti per migliorare le nostre vite con prodotti e servizi nonché contatti umani migliori e più frequenti. Sfortunatamente, questi cambiamenti offrono anche nuove opportunità ai criminali. Sappiamo per esperienza che questi avversari possono essere intelligenti, ben equipaggiati e creativi: troveranno e sfrutteranno qualsiasi punto debole tecnologico o umano nei nostri sistemi di difesa. Questi sviluppi sono significativi anche per gli assicuratori che sottoscrivono questi rischi emergenti.

La questione è particolarmente cruciale per le piccole e medie imprese (PMI) in Svizzera, spesso all’avanguardia nello sviluppo e nell’innovazione del mercato, ma con risorse limitate da dedicare alla sicurezza informatica. Gli ultimi anni hanno dimostrato quanto queste imprese siano nel mirino dei criminali informatici. In Allianz Suisse, abbiamo sempre sostenuto i nostri clienti con prodotti eccellenti, servizi su misura e soluzioni innovative: questo nuovo studio è in linea con il nostro primato nell’ambito dell’innovazione.

L’atteggiamento dei dipendenti di fronte ai rischi informatici è una componente cruciale della protezione generale e del meccanismo di risposta di un’impresa. L’Università di Zurigo di Scienze Applicate (ZHAW) ha sviluppato un interessante focus di ricerca sul comportamento del cliente in ambito assicurativo e, da parte nostra, siamo lieti di partecipare a questo progetto. In particolare, il presente studio ha individuato interessanti insight comportamentali e culturali negli atteggiamenti dei dipendenti delle PMI e ha formulato raccomandazioni chiare e mirate per le imprese stesse e i loro fornitori di tecnologie e assicurazioni.

Spero troviate questa pubblicazione informativa e stimolante.

Severin Moser

CEO, Allianz Suisse

Management Summary

Gli attacchi informatici rappresentano un problema sempre più rilevante per le PMI svizzere: circa un terzo di esse è già stato vittima di attacchi informatici e il 4% è stato successivamente ricattato. Questi problemi sono iniziati perlopiù con attacchi di phishing, in seguito ai quali elementi criminali hanno ottenuto accesso al sistema IT sfruttando un errore o una disattenzione dei dipendenti. Abbiamo intervistato numerosi dipendenti di PMI svizzere per comprendere in quale modo i loro atteggiamenti nei confronti degli attacchi informatici possano influire su questa vulnerabilità e per elaborare suggerimenti pratici per interventi correttivi. Le interviste sono state condotte utilizzando metafore profonde allo scopo di comprendere i fattori culturali ed emotivi nascosti del comportamento, piuttosto che le componenti razionali visibili. Abbiamo elaborato tre raccomandazioni per fare leva sulla cultura proattiva delle PMI e ridurre la loro dipendenza da fornitori terzi: aumentare la consapevolezza, responsabilizzare i dipendenti ed esercitarsi a lavorare in modalità di ripristino.

Sommario

Introduzione

1.1. RISCHI INFORMATICI E PMI SVIZZERE

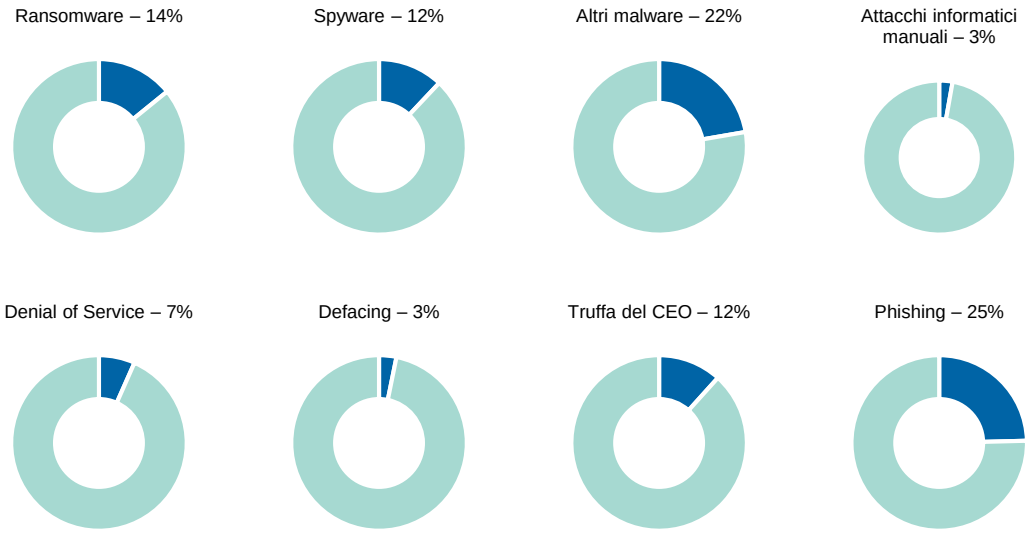
Violazioni dei dati o della sicurezza, spionaggio, attacchi hacker, ransomware e denial of service nonché errori dei dipendenti sono le principali cause degli incidenti informatici, eventi ormai sempre più comuni e costosi. Questa evoluzione è evidenziata dall'Allianz Risk Barometer (2020) a cui hanno contribuito oltre 2700 esperti di rischio a livello mondiale: gli incidenti informatici hanno soppiantato l'interruzione d'esercizio in vetta alla classifica dei rischi. La crescente interconnessione dell'economia si traduce in una sempre maggiore vulnerabilità delle imprese agli attacchi informatici e le notizie di spettacolari attacchi hacker e furti di dati sono in aumento. Le imprese sono esposte al rischio di danni milionari, danni di immagine e persino di interruzione di esercizio, eventi che mettono a repentaglio la loro esistenza e che possono verificarsi qualora criminali informatici rubino dati, insinuino programmi dannosi nelle reti o paralizzino i server (Allianz, 2020). Severin Moser, CEO di Allianz Suisse, stima che le conseguenze del crimine informatico costino all'economia globale oltre 600 miliardi di dollari USA ogni anno (NZZ, 2019). Tuttavia, è difficile quantificare nel dettaglio l'evoluzione di questo fenomeno a causa della mancanza di dati affidabili e di un numero elevato di casi non denunciati. Il Gruppo di lavoro Cyber Risk dell'Associazione svizzera d'Assicurazioni stima un costo annuo di 9,5 miliardi di franchi solo in Svizzera, e questo dato è in aumento (SIA, 2018).

Le imprese di piccole e medie dimensioni (PMI), vale a dire le imprese con un massimo di 250 dipendenti, rappresentano oltre il 99% di tutte le imprese e offrono due terzi dei posti di lavoro in Svizzera (Ufficio federale di statistica, 2020). Rivestono un ruolo cruciale nell'economia svizzera e sono fortemente colpite dagli attacchi informatici. Circa un terzo delle PMI svizzere è già stato vittima di attacchi informatici e il 4% è stato successivamente ricattato (Mändli Lerch e Repic, 2017). Anche se i dati delle imprese più piccole sono poco interessanti per i criminali informatici, queste imprese continuano a essere bersagli appetibili per due motivi: innanzitutto, per estorcere un riscatto utilizzando ransomware e, in secondo luogo, come varco per attaccare le imprese più grandi che lavorano con le PMI (Heer, 2020). La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione, integrata nel Centro nazionale per la cibersicurezza (NCSC) nel luglio 2020, ha segnalato un maggiore rischio di attacchi ransomware nella prima parte del 2020 (MELANI, 2020a). Questa minaccia è in continuo aumento, si è quadruplicata nel 2019 ed è ora uno degli incidenti informatici più comuni (Trustwave, 2020). Vi sono numerosi esempi di imprese svizzere vittime di attacchi ransomware e quattro di esse sono trattate nel capitolo seguente.

Studi recenti hanno iniziato ad analizzare in maggior dettaglio gli attacchi informatici alle PMI nei Paesi confinanti. Dreissigacker et al. (2020) stima ad esempio che in Germania dal 40% al 50% delle PMI con oltre 10 dipendenti è esposto ogni anno ad attacchi informatici, anche se la maggior parte di essi vengono neutralizzati e non causano alcun danno. Questo dato è più basso, seppur non in modo significativo, di quello delle imprese più grandi: ogni anno dal 50% al 60% di esse è infatti bersaglio di un attacco. Il presente studio analizza inoltre il tasso annuo di ciascuna delle principali categorie di attacchi informatici, come mostrato nella Figura 1. Le PMI possono aspettarsi un attacco di phishing ogni quattro anni e uno ransomware ogni sette, approssimativamente in linea con la frequenza nelle imprese più grandi. Dall'altra parte, il numero di «truffe del CEO» e di attacchi informatici manuali è considerevolmente inferiore per le PMI, forse in ragione del maggiore coinvolgimento diretto del CEO nelle imprese più piccole e del guadagno finanziario potenzialmente inferiore. Studi condotti in altri Paesi europei riportano risultati analoghi, ma a volte con scostamenti significativi, anche se è difficile fare un confronto diretto in ragione delle metodologie di ricerca e dei meccanismi di comunicazione differenti. In linea generale, questi studi confermano tuttavia la significativa minaccia generale derivante per le PMI dagli attacchi informatici.

Figura 1: Tasso annuo stimato degli attacchi informatici alle PMI

TASSO STIMATO DEGLI ATTACCHI INFORMATICI ALLE PMI PER ANNO E TIPOLOGIA IN GERMANIA 2018/2019



Fonte: Dreissigacker et al. (2020)

Gli attori informatici «maligni» adeguano regolarmente gli attacchi di ingegneria sociale, in particolare di phishing, ai principali eventi di attualità, ad es. eventi sportivi o l'attuale pandemia da COVID-19. Tuttavia, praticamente tutte le più comuni famiglie di malware vengono attualmente diffuse utilizzando come esca il COVID-19, nella maggior parte dei casi attraverso e-mail contenenti un allegato infetto o un link a un sito web infetto (MELANI, 2020b). Il numero di e-mail di phishing è cresciuto durante la pandemia; a titolo esemplificativo, gli scammer che impersonano dipendenti dell'Organizzazione mondiale della sanità (OMS) hanno preso a bersaglio i fondi di emergenza per le vittime del COVID-19 e hanno attirato gli utenti verso siti web dannosi utilizzando annunci pubblicitari falsi (de Moura et al., 2020). Gli attacchi di phishing hanno inoltre puntato specificamente al diverso ambiente di lavoro. Inizialmente, molti utenti non avevano familiarità con i software collaborativi e per conferenze e con i messaggi inviati da queste piattaforme, il che ha reso più difficile riconoscere le e-mail di phishing (MELANI, 2020b). Numerosi articoli mettono in luce le vulnerabilità delle imprese dovute a errori umani e la rilevanza degli attacchi di phishing. Sebbene l'infrastruttura tecnica rimanga un fattore cruciale, i dipendenti sono spesso vittime di schemi ingegnosi ed espongono le proprie imprese al rischio di frode o malware (Pugnetti et al., 2019). Le PMI svizzere sono generalmente protette in misura insufficiente contro i rischi informatici, in particolare in termini di servizi di mitigazione e ripristino (Pugnetti e Schneebeli, 2020).

L'obiettivo di questa ricerca è comprendere le potenziali vulnerabilità dovute alle percezioni del crimine informatico da parte dei dipendenti e alla cultura societaria delle PMI, allo scopo di elaborare suggerimenti per meccanismi di difesa fruibili per le imprese nonché sviluppare interventi formativi e servizi che potranno essere forniti da terzi.

1.2. ESEMPI DI IMPORTANTI ATTACCHI INFORMATICI IN SVIZZERA

Sono stati numerosi i casi di attacchi informatici ai danni delle PMI svizzere riportati dai media. Quattro attacchi sono stati particolarmente rilevanti per le imprese intervistate in questo studio e sono descritti più in dettaglio qui di seguito.

1.2.1. OFFIX AG, 2019

OFFIX AG, società operante nel settore delle attrezzature per uffici con un organico di 250 dipendenti e un fatturato di 300 milioni di franchi svizzeri (Papedis, n.d.), è stata vittima di un attacco ransomware il 15 maggio 2019 (Jochum, 2019). Si ipotizza che un hacker abbia intercettato la corrispondenza e-mail con un cliente sostituendosi a quest'ultimo nello scambio. Un dipendente dell'impresa ha quindi ricevuto una richiesta di certificazione e ha cliccato sul link fornito, permettendo al virus di infettare il sistema IT dell'impresa. Le prime irregolarità sono state

rilevate il giorno successivo; il 17 maggio era ormai chiaro che, in termini di IT, «nulla era rimasto»: banche dati cancellate e numerosi server riportati alle impostazioni di fabbrica. Anche molte interfacce cliente per l'inserimento degli ordini erano state cancellate e OFFIX aveva perso traccia degli ordini in entrata e delle vendite. Per la decrittazione, il riscatto richiesto era di 45 bitcoin (per un controvalore in quel momento di 350 000 franchi svizzeri). L'impresa ha incaricato uno specialista esterno in crimini informatici e ha informato sia la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) sia la polizia. Prima di andare completamente offline, l'impresa ha chiesto ai propri clienti di piazzare i nuovi ordini via telefono, fax oppure utilizzando i nuovi indirizzi e-mail creati. Fortunatamente, l'hacker aveva commesso un errore e, in più, solo poche settimane prima uno specialista IT aveva salvato un'applicazione importante su un disco rigido esterno. OFFIX è quindi riuscita a ripristinare parte della sua banca dati e a ricostruire i suoi sistemi IT (Severin, 2019). Secondo il CEO, Martin Kelterborn, il danno economico non è quantificabile, ma l'attacco è stato «molto, molto costoso» (Jochum, 2019).

1.2.2. Swisswindows, 2019

Nel maggio 2019 Swisswindows, produttore di serramenti e infissi con circa 170 dipendenti (Borkert, 2020), è stata costretta a sospendere la produzione per oltre un mese a seguito di un attacco ransomware. Probabilmente gli hacker erano penetrati nella rete dell'impresa utilizzando un'e-mail apparentemente irrilevante e avevano crittografato i dati della società. Gli ordini non erano più visibili e i dipendenti non avevano accesso ai dati di clienti e macchine. L'impresa era paralizzata. Un'impresa IT esterna aveva effettuato backup quotidiani dei dati, ma i file di backup erano collegati al server dell'impresa e quindi anch'essi inaccessibili. Nonostante il cospicuo riscatto in bitcoin richiesto dai criminali informatici per restituire i dati, l'impresa ha deciso di non pagare, preferendo investire nella sostituzione della propria infrastruttura IT, operazione comunque necessaria (Klein, 2020). Tuttavia, nel febbraio 2020, i dipendenti sono stati informati che l'impresa era in fallimento. L'attacco informatico aveva accelerato il declino già in atto delle attività core dell'impresa, contribuendo pertanto alla sua rovina (SRF, 2020).

1.2.3. Meier Tobler, 2019

Meier Tobler, società di domotecnica con un fatturato di 500 milioni di franchi svizzeri e circa 1300 dipendenti (Meier Tobler, 2020), è stata vittima di un attacco ransomware nel luglio 2019 (Luzerner Zeitung, 2019). Gli hacker hanno ottenuto accesso tramite un allegato e-mail che conteneva malware (Schäppi, 2020). Il sistema SAP centrale, il sistema di controllo del magazzino, la telefonia fissa, il sito web e tutti gli indirizzi e-mail hanno smesso di funzionare (Lüscher e Niedermann, 2019). L'impatto sulle vendite e sui profitti è stato considerevole, come riferito nel comunicato stampa dell'impresa:

> sebbene siano state attivate le procedure di emergenza predisposte e sia stata realizzata in breve tempo un'infrastruttura provvisoria, non è stato possibile evitare l'interruzione temporanea delle consegne, con un conseguente immediato crollo delle vendite nell'attività commerciale pari a circa 5 milioni di franchi svizzeri. Un'ulteriore perdita di vendite di entità analoga è stata successivamente registrata nell'attività di generazione di calore a causa dell'indisponibilità dei sistemi IT.

I costi supplementari diretti per la gestione dall'attacco hanno intaccato gli utili annui 2019 per 1 milione di franchi svizzeri. Da allora, l'impresa ha ricostruito la sua infrastruttura IT secondo i più recenti criteri in materia di sicurezza (Meier Tobler, 2020).

1.2.4. Stadler Rail, 2020

Stadler Rail produce veicoli ferroviari e, con 11 000 dipendenti e ricavi globali per oltre 3,2 miliardi di franchi svizzeri (Stadler Rail, 2020a), non rientra nella categoria delle PMI. Tuttavia, questo attacco informatico è stato menzionato dalle persone intervistate per questo studio ed è quindi rilevante. Il 7 maggio 2020 «la rete IT di Stadler ha subito un attacco con malware. La società ha avviato immediatamente le misure di sicurezza necessarie coinvolgendo le autorità responsabili. È in corso un'indagine dettagliata al riguardo.» (Stadler Rail, 2020b). Gli autori dell'attacco hanno ricattato Stadler minacciando la pubblicazione dei dati rubati e chiedendo il pagamento di sei milioni di dollari USA in bitcoin. La società ha confermato in una dichiarazione a inside-it.ch che «si tratta di documenti e dati confidenziali rubati a Stadler a seguito di attività criminali» (Anz, 2020). Stadler si è rifiutata di pagare il riscatto. I criminali hanno quindi pubblicato alcuni record di dati per aumentare la pressione sulla società, e successivamente hanno divulgato ulteriori dati poiché la società continuava a rifiutarsi di pagare (Griesser Kym, 2020). Tuttavia, Stadler non è mai stata disposta né a rispondere alle richieste dei ricattatori né a effettuare pagamenti – e «mai lo farà» (Anz, 2020).

1.3. PROTEZIONE DELLA VOSTRA IMPRESA

Tutte le imprese devono definire quali rischi desiderano evitare, ridurre, trasferire o sostenere esse stesse nell'ambito del proprio processo decisionale relativo alla gestione dei rischi. In questo contesto, è essenziale comprendere quali sono le soluzioni assicurative disponibili e quali di queste avrebbero offerto un certo grado di protezione nei casi summenzionati. Gli attacchi informatici possono essere fonte di perdite dirette, quali i costi per il ripristino dei dati, e interrompere la normale attività d'impresa. Le polizze assicurative standard sulla proprietà coprono i danni alla proprietà e la conseguente interruzione dell'attività se la causa del danno (ad es. un incendio) è assicurata. Tuttavia, con un attacco informatico non vi è necessariamente un danno alla proprietà ed è quindi raro che si possa ricorrere a questo tipo di assicurazione. Inoltre, le imprese potrebbero dover far fronte a pretese di responsabilità verso terzi dopo l'attacco informatico, a titolo esemplificativo in caso di fuga o cancellazione dei dati dei clienti. La normale assicurazione per danni contro terzi copre le pretese derivanti da lesioni personali e danni alla proprietà e le conseguenti perdite finanziarie. L'assicurazione di responsabilità civile verso terzi che copre la mera perdita finanziaria è normalmente destinata a specifici gruppi professionali e non è pertanto ampiamente diffusa.

Le classiche polizze assicurative commerciali hanno in comune il fatto che non coprono specificamente i rischi informatici. In determinate circostanze, il danno e gli effetti di un attacco informatico sono assicurati attraverso questi prodotti, tuttavia queste polizze non sono espressamente concepite per rendere il rischio informatico controllabile per le imprese. Si tenga presente che fino all'avvento dell'era Internet non esistevano rischi informatici e che le prime coperture del rischio informatico sono state create a cavallo del nuovo millennio per fare fronte a questa nuova minaccia. In Svizzera, le prime polizze di rischio informatico sono state introdotte dagli assicuratori internazionali nel 2015 e il lancio di soluzioni assicurative complete per le PMI è avvenuto nel 2017. Queste soluzioni comprendono solitamente la responsabilità civile verso terzi, le perdite dirette e la gestione dell'emergenza e coprono anche il crimine informatico / l'ingegneria sociale e la protezione legale per i rischi informatici. Questi prodotti sono focalizzati sia sugli attacchi informatici sia sulla condotta inadeguata dei dipendenti e sulle violazioni della protezione dei dati. Oltre al rimborso dei danni subiti, le imprese possono avvalersi di una rete di specialisti in tecnologia dell'informazione, comunicazione d'emergenza e protezione legale per calcolare l'entità del danno, accelerare la riparazione ed evitare o ridurre il danno d'immagine per l'impresa. La Tabella 1 fornisce una panoramica sulle coperture assicurative Cyber più diffuse attualmente disponibili (Pugnetti et al., 2019).

Tabella 1: Coperture assicurative Cyber attuali

COPERTURE ASSICURATIVE CYBER ATTUALI

Responsabilità civile verso terzi Rivendicazioni e richieste da parte di terzi	- Violazioni della protezione dei dati - Perdita di dati - Appropriazione indebita/perdita di funzionalità - Comunicazione digitale - Pagamenti elettronici/sanzioni contrattuali - Inoltro di malware
Perdite dirette Perdite subite dal titolare della polizza	- Costi di ripristino - Interruzione d'esercizio - Furto per attacco informatico - Ricatto informatico - Procedure ufficiali di protezione dei dati
Gestione dell'emergenza Servizi in caso di rivendicazione	- Servizi forensi - Costi di informazione - Comunicazione dell'emergenza - Costi dell'emergenza
Protezione legale Controversie relative a rischi informatici	- Diritto contrattuale - Violazione dei diritti della personalità - Abuso di identità - Abuso di carte di credito e informazioni del conto - Dominio Internet
Crimine informatico – Ingegneria sociale Perdite finanziarie derivanti da frode di terzi	- Truffa mediante assunzione di falsa identità - Truffa mediante deviazione dei flussi di cassa - Truffa mediante uso di identità false

1.4. INTERVISTE CON L'UTILIZZO DI METAFORE PROFONDE

La ricerca di mercato è stata a lungo incentrata sulla comprensione delle strutture cognitive, ossia dei sistemi di credenze, e ha dato priorità alla struttura rispetto al contenuto (Olson e Reynolds, 1983). Tuttavia, un modo migliore per descrivere e rappresentare i consumatori è il modello mentale, che consente di ottenere rappresentazioni non basate sulle credenze, fra cui atteggiamenti, sentimenti, immagini, ricordi, valori, ecc. (Christensen e Olson, 2002). Questo approccio è inoltre maggiormente in linea con l'orientamento attuale delle neuroscienze cognitive, secondo cui i pensieri sono basati su immagini (Damasio, 1994). Gli strumenti di ricerca ed elicitazione si sono evoluti per cercare di catturare la crescente complessità dei modelli mentali. Uno di questi strumenti è la tecnica di elicitazione della metafora di Zaltman (ZMET). In particolare, l'ipotesi teorica alla base della ZMET è l'importanza del contenuto tacito inconscio, vale a dire delle conoscenze nascoste, e l'importanza delle immagini nei modelli mentali. La ZMET utilizza immagini per aiutare gli informatori a individuare e comunicare contenuti (Zaltman, 1997) ed è stata utilizzata per elicitare i fattori emotivi più profondi del comportamento e delle scelte dei consumatori (Zaltman e Zaltman, 2008).

La tecnica è strutturata in tre fasi. Innanzitutto, si chiede ai rispondenti di pensare a un argomento e di selezionare immagini che rappresentano i loro pensieri e le loro sensazioni al riguardo. Si intervistano quindi i rispondenti per comprendere i significati che hanno attribuito alle immagini e si definiscono le connessioni alle idee sovraordinate utilizzando tecniche di laddering. Infine, si generano i risultati creando mappe di consenso dei costrutti centrali e ampi temi di significato (Christensen e Olson, 2002). Il risultato finale è una serie di temi che gli intervistati associano all'argomento oggetto della ricerca. Non vi è alcun tentativo di generare risultati statisticamente significativi; al contrario, l'attenzione è incentrata sul portare alla luce informazioni nascoste. La tecnica è stata utilizzata in numerosi studi, fra gli altri anche dagli autori del presente studio, per progetti di consulenza e in uno studio pubblicato finalizzato all'analisi dell'esperienza di nuovi clienti assicurativi. A titolo esemplificativo, in quello studio i nuovi clienti hanno chiaramente segnalato la propria frustrazione nei confronti del gergo tecnico del settore e la mancanza di familiarità con i brand assicurativi (Pugnetti e Bekaert, 2018).

1.5. METODOLOGIA

Abbiamo reclutato tre PMI con attività correlate all'ingegneria meccanica e condotto interviste utilizzando metafore profonde con 17 volontari, rappresentanti di un'ampia gamma di profili di dipendenti nell'organizzazione, fra cui management, personale amministrativo, addetti della produzione e dipendenti fuori sede. Agli intervistati è stato chiesto di scegliere 3-5 immagini che descrivessero le sensazioni provate di fronte alla notizia di attacchi informatici (Tabella 2). I partecipanti sono stati successivamente intervistati sul significato delle immagini scelte.

Tabella 2: Domanda della ricerca

Domanda della ricerca	Cosa prova quando sente parlare di attacchi informatici?

Le interviste sono state condotte nel settembre 2020, congiuntamente dai due autori, e presso la sede di ciascuna impresa. La durata di ciascuna intervista è stata di circa un'ora, a seconda del numero di immagini utilizzate e delle domande di follow-up scaturite dalla discussione. I risultati sono stati quindi discussi in una serie di workshop e consolidati per generare le mappe di consenso, quindi sono stati presentati i temi principali. Questi temi verranno trattati nei paragrafi seguenti utilizzando le immagini originali e la lingua delle interviste. In alcuni casi, le immagini originali sono state sostituite con immagini analoghe per questioni di licenza.

Gli intervistati si sono descritti come riepilogato nella Tabella 3:[1]

Tabella 3: Autodescrizione degli intervistati

AUTODESCRIZIONE DEGLI INTERVISTATI

1	Incline ad aiutare, non vuole ferire nessuno	10	Amichevole, ha a cuore gli altri
2	Persona con visione positiva	11	Persona aperta, ma attenta
3	Persona tranquilla e riflessiva	12	Persona «con i piedi per terra», ma aperta
4	Persona contenta della vita	13	Prudente
5	Persona tranquilla, non cerca guai	14	Indole buona, flessibile
6	Persona leale, buona ascoltatrice	15	Persona conservatrice, ma aperta
7	Persona positiva	16	Persona responsabile
8	Persona orientata agli obiettivi	17	Persona comunicativa e curiosa
9	Persona tranquilla e affidabile		

[1] Per tutelare la riservatezza, l'ordine non corrisponde a quello delle interviste

Risultati

Le interviste hanno messo in luce diversi fili conduttori comuni. Temi ricorrenti sono stati la natura geopolitica degli attacchi informatici, i collegamenti al crimine organizzato e la motivazione di carattere finanziario. L'hacker è stato descritto come un «professionista» con competenze specifiche e attrezzature eccellenti e non necessariamente sempre come una forza negativa. In linea generale, gli intervistati si sentivano incapaci di riconoscere gli attacchi informatici o proteggersi da essi. Di conseguenza si sentivano vulnerabili, ma comunque consapevoli dei pericoli rappresentati dagli attacchi di phishing e hanno riconosciuto l'esito potenzialmente catastrofico degli attacchi informatici. Molti hanno citato il recente caso di Meier Tobler. Al contempo, non si sentivano abbastanza importanti né consideravano la loro società abbastanza grande da diventare un possibile bersaglio degli attacchi. In caso di attacco, farebbero affidamento su fornitori di servizi esterni per risolvere il problema. Infine, hanno manifestato un atteggiamento molto positivo verso una risoluzione dei problemi e una ricerca di soluzioni indipendente, compreso il ricorso, laddove necessario, a metodi vecchio stampo..

Tabella 4: temi comuni ed etichette delle immagini

	TEMA	ETICHETTE DELLE IMMAGINI
1	**Politica globale e crimine organizzato**	Servizi segreti Uomo nell'ombra Il bottino
2	**Il mito dell'hacker**	L'hacker Una postazione di lavoro super Furfante o benefattore?
3	**Sentirsi impotente**	Calamita di dati Manipolazione sociale Domande senza risposta
4	**Sentirsi vulnerabile**	Sotto controllo Cautela! Phishing
5	**Esito catastrofico**	Forma di effrazione moderna Attacco al nostro fornitore Spero di no!
6	**Non mi riguarda**	Il mondo intero Paura Assistenza
7	**Proattivo e impegnato**	Nebbia Pianificazione Come ai vecchi tempi

Queste risposte così sfaccettate a una domanda relativamente semplice indicano un modo di pensare sofisticato. Ciò ha consentito di individuare numerose aree di miglioramento e di sviluppare raccomandazioni chiare per le PMI svizzere e i loro fornitori di servizi.

2.1. POLITICA GLOBALE E CRIMINE ORGANIZZATO

Gli intervistati considerano gli attacchi informatici parte di uno schema di intrighi internazionali e giochi politici e globali ad alto rischio. Pur avendo citato attacchi informatici verificatisi in ambienti vicini a loro o alla loro impresa (perlopiù Meier Tobler, come indicato in precedenza), gli intervistati hanno generalmente collocato gli attacchi informatici nel contesto di conflitti politici internazionali. Alcuni degli esempi citati con maggiore frequenza sono le elezioni USA e il sospetto di interferenze russe, così come il terrorismo. Tuttavia, la Svizzera viene considerata un porto sicuro, con un sistema politico più stabile. Tuttavia, gli intervistati erano consapevoli del fatto che il crimine organizzato è la potente forza coordinatrice dietro gli attacchi informatici. Affinché gli attacchi abbiano successo, è necessario un ampio coordinamento di svariati specialisti e fonti di dati nel tempo, cosa che richiede organizzazione. Tra le motivazioni degli attacchi informatici è stato indicato il guadagno economico, e occasionalmente la sete di potere. Sebbene la componente politica possa far sembrare il crimine informatico relativamente più remoto, i motivi di carattere finanziario e criminale lo rendono più vicino, e quindi più riconoscibile e rilevante per gli intervistati.

Figura 2: Servizi segreti

SERVIZI SEGRETI

Sono in atto grandi mutamenti nella struttura del potere internazionale e non importa se questo implica la morte di alcune persone. Le cose sono però diverse in Svizzera, l'intero sistema è più sicuro.

Figura 3: Uomo nell'ombra

UOMO NELL'OMBRA

Non si sa chi sia questa persona, ma è certamente il crimine organizzato, la mafia. Si può chiamare la polizia o farsi da parte, ma è troppo pericoloso affrontarlo direttamente.

Figura 4: Il bottino

IL BOTTINO

Denaro, molto denaro. In fin dei conti, è solo una questione di denaro.

La tendenza ad associare il crimine informatico alle grandi forze geopolitiche, ipotizzando al contempo che la Svizzera sia un porto sicuro, potrebbe rendere le PMI svizzere più vulnerabili. I dipendenti potrebbero essere meno vigili di quanto dovrebbero. Tuttavia, riconoscere il ruolo del crimine organizzato e le motivazioni finanziarie ad esso associate è un segnale positivo.

2.2. IL MITO DELL'HACKER

La persona che esegue l'attacco vero e proprio è stata spesso identificata con la parola inglese «hacker» e descritta come una figura incappucciata dietro a un computer. Tutti gli intervistati hanno affermato che molto probabilmente un hacker non ha questo aspetto e potrebbe essere sia un uomo sia una donna. Agli hacker vengono attribuiti una notevole competenza tecnica e spazi lavorativi ben attrezzati – di fatto, migliori di quelli delle loro vittime designate. Gli hacker non vengono considerati come una forza negativa in termini assoluti. Spesso sono stati anche definiti come una potenziale forza positiva – in grado per esempio di smascherare gruppi di pedofili e/o attività finalizzate alla corruzione. Questa differenziazione del giudizio sulla pirateria informatica consente agli hacker etici di sondare le difese di un'impresa in cambio di una remunerazione lecita.

Figura 5: L'hacker

L'HACKER

Connesso a numerose persone in molti Paesi. Anonimo e spaventoso.

Figura 6: Una postazione di lavoro super

UNA POSTAZIONE DI LAVORO SUPER

Non so perché ha così tanti dispositivi, ma li usa tutti. Può hackerare persino imprese preparate e ben protette.

Figura 7: Furfante o benefattore?

FURFANTE O BENEFATTORE?

Sono neutrale al riguardo. Potrebbe essere un criminale o un whistleblower.

Le risposte degli intervistati hanno confermato la consapevolezza in merito alla complessità degli attacchi informatici e alle motivazioni sottostanti, nonché ai potenziali vantaggi dell'attività di whistleblowing. Tuttavia, associando gli attacchi alle grandi forze geopolitiche, i dipendenti rischiano di relegare gli attacchi informatici a un contesto in cui essi e le loro PMI sono «troppo insignificanti» per attrarre attenzioni indesiderate – aumentando automaticamente la loro vulnerabilità.

2.3. SENTIRSI IMPOTENTE

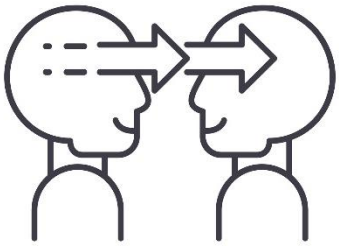
Gli intervistati hanno parlato apertamente dell'opacità degli attacchi informatici e della loro incapacità di comprenderne la dinamica. I dati possono essere sottratti senza che nessuno se ne accorga, come un magnete che attrae i metalli ferrosi. Gli atteggiamenti nei confronti degli attacchi informatici possono essere influenzati e manipolati nel tempo senza che nessuno se ne accorga. Numerose domande rimangono senza risposta – chi si cela dietro gli attacchi e perché, nonché come si dovrebbe reagire durante o dopo un attacco. Ad oggi, la sensazione generale è di impotenza nei confronti degli attacchi informatici. Non è un segnale positivo, perché scoraggia il coinvolgimento attivo e l'adozione di misure di difesa adeguate. Dall'altra parte, le campagne informative e i programmi di formazione atti a migliorare le conoscenze e la consapevolezza dovrebbero trovare un pubblico interessato e motivato.

Figura 8: Calamita di dati

CALAMITA DI DATI

I dati possono essere estratti da una rete così come una calamita attira ogni cosa verso di sé.

Figura 9: Manipolazione sociale



MANIPOLAZIONE SOCIALE

Vi è un abuso di fiducia. Se un dipendente non presta attenzione, può fare un errore e perdere il proprio posto di lavoro.

Figura 10: Domande senza risposta

DOMANDE SENZA RISPOSTA

Perché lo ha fatto? Cosa possiamo fare? Non possiamo fornire risposte o trovare soluzioni da soli.

Sfortunatamente, la sensazione di impotenza genera passività, sia nella preparazione agli attacchi informatici sia nella risposta ad essi. La responsabilità per la protezione informatica viene quindi trasferita a soggetti terzi specializzati e più esperti, facendo venire meno la centralità del ruolo di ciascun dipendente nella protezione dell'impresa. Sussiste la necessità di sviluppare programmi di formazione specifici per aumentare la consapevolezza in termini di comportamenti rischiosi e le conoscenze degli strumenti disponibili al fine di incentivare un atteggiamento proattivo dei dipendenti.

2.4. SENTIRSI VULNERABILE

Gli intervistati sanno di essere osservati quando sono online. Non amano questa sensazione, tanto meno il fatto di non poter impedire che ciò accada. Sanno che i criminali informatici possono abusare della loro fiducia per danneggiare le imprese per cui lavorano e che questa situazione può esporli a conseguenze dirette e indirette. Un intervistato ha paragonato questa situazione all'aprire la porta a uno sconosciuto, che potrebbe entrare nell'edificio e rubare delle attrezzature. Inoltre, abbiamo tutti una vita privata e comportamenti di cui non andremmo fieri se venissero resi pubblici o condivisi con un pubblico più ampio. Questo ci rende vulnerabili e incapaci di difenderci da un attacco. Gli hacker sfruttano la nostra vulnerabilità e ottengono accesso mediante attacchi di phishing progettati per prenderci alla sprovvista.

Questa sensazione di vulnerabilità è spiacevole; per questo, la normale reazione umana consiste nell'evitare di pensarci. Come ha affermato uno degli intervistati, «se pensassimo a tutto ciò che potrebbe succedere, non andremmo mai online.» Tuttavia, la consapevolezza della gravità degli attacchi di phishing è un'indicazione incoraggiante del livello di conoscenza di cui dispongono già i dipendenti in merito agli attacchi informatici e pertanto un punto di riferimento utile nelle sessioni di formazione.

Figura 11: Sotto controllo

SOTTO CONTROLLO

Qualcuno osserva questa giovane donna alle spalle. E lei non può impedirlo. Non mi piace provare questa sensazione.

Figura 12: Cautela!

CAUTELA!

Questa persona viene ricattata – qualcosa della sua vita privata passata è stata resa pubblica. Ha fcommesso un errore su una piattaforma di social media.

Figura 13: Phishing

PHISHING

I dati vengono rubati tramite attacchi di phishing. Si può cercare di proteggersi con un antivirus e altri programmi, ma questi non serviranno contro i professionisti.

La consapevolezza di essere osservati è un segnale positivo e può portare a tenere maggiormente in considerazione i rischi e a tenere un comportamento più prudente quando si è online. La comprensione della minaccia specifica rappresentata dal phishing è importante e incoraggiante. Il phishing è il modo più insidioso di sfruttare le vulnerabilità umane, perché raccoglie informazioni e consente agli hacker di agire inosservati e a lungo prima di colpire. Le misure per contrastare in modo efficace il phishing dovrebbero includere l'educazione delle persone a rispondere alle richieste online con la dovuta cautela.

2.5. ESITO CATASTROFICO

I rispondenti considerano gli attacchi informatici semplicemente come un'altra forma di effrazione; al pari di un'effrazione fisica, anche un tentativo fallito è dannoso e inquietante. L'incidente che ha paralizzato Meier Tobler, un fornitore, ha fatto emergere la consapevolezza di quanto un attacco di questo tipo possa rivelarsi catastrofico. Nonostante, alla fine, l'impresa sia riuscita a ripristinare la propria operatività, il danno economico è stato significativo e vi sono state ripercussioni anche per gli intervistati stessi nella loro attività quotidiana. È interessante notare che, pur mostrando pieno sostegno e comprensione per i problemi del loro partner commerciale, dalle risposte è emersa un'evidente irritazione e insofferenza per l'incapacità dell'impresa di risolvere il problema in tempi più rapidi. In linea generale, gli intervistati hanno mostrato una solida consapevolezza della possibilità di paralisi dei sistemi IT e dell'impatto catastrofico che una simile circostanza potrebbe avere sull'attività.

Figura 14: Forma di effrazione moderna

FORMA DI EFFRAZIONE MODERNA

L'attacco informativo è semplicemente una moderna forma di effrazione. La normale protezione non è sufficiente per impedire un accesso non autorizzato e i danni si verificano a prescindere da ciò che accade – come minimo ci sarà una finestra rotta.

Figura 15: Attacco al nostro fornitore

ATTACCO AL NOSTRO FORNITORE

Il nostro fornitore era completamente automatizzato ed è stato attaccato. Non è riuscito a mantenere la propria operatività e ha perso milioni. La stessa cosa potrebbe succedere a noi.

Figura 16: Spero di no!

SPERO DI NO!

Le cose potrebbero inaspettatamente andare storte.

La consapevolezza delle potenziali conseguenze degli attacchi informatici rappresenta un buon punto di partenza per i programmi di formazione. È emerso chiaramente che l'accondiscendenza nei confronti dei partner commerciali colpiti da attacchi informatici è limitata: questo significa che un'impresa colpita dispone di un margine di ripristino relativamente breve prima di subire conseguenze a lungo termine sulle relazioni commerciali. In caso di attacco, è pertanto fondamentale ripristinare l'operatività commerciale il più rapidamente possibile.

2.6. NON MI RIGUARDA

Sebbene gli intervistati abbiano riconosciuto le proprie vulnerabilità, ritenevano di valere troppo poco per poter attirare attenzioni indesiderate. In certa misura, questo modo di pensare veniva trasposto anche all'impresa di cui erano dipendenti. Le PMI erano considerate troppo piccole rispetto alle multinazionali. Le interviste hanno evidenziato inoltre la percezione che i pericoli possano essere sovrastimati e che il timore di un attacco possa dare adito a interventi non necessari e potenzialmente dannosi. Tuttavia, in caso di attacco all'impresa, i fornitori di servizi esterni fornirebbero le soluzioni e le conoscenze per risolvere il problema, così come una buona infermiera in un ospedale ben attrezzato si prende cura dei pazienti malati. Questo paragone, in particolare, suggerisce una potenziale debolezza sistemica. Ci affidiamo prontamente alle cure di medici e infermieri, escludendo la possibilità di auto-medicarci in caso di malattia. Analogamente, potremmo ipotizzare che sia automaticamente meglio lasciare la sicurezza digitale unicamente nelle mani degli specialisti.

Figura 17: Il mondo intero

IL MONDO INTERO

Non appena si collega la spina, il mondo intero è connesso e abbiamo accesso a tutte le conoscenze. Un cambiamento molto positivo.

Figura 18: Paura

PAURA

Timore infondato che succeda qualcosa online, anche se siamo relativamente sicuri. Troppa protezione non è necessaria.

Figura 19: Assistenza

ASSISTENZA

Un'impresa sotto attacco si sente come «ammalata» e ha bisogno di esperti esterni e attrezzature specializzate per poter guarire.

La convinzione di essere troppo piccoli e insignificanti per essere bersaglio dei criminali informatici è forse l'aspetto più preoccupante emerso dalle risposte di molti dipendenti delle PMI. Anche se i singoli individui potrebbero non essere il bersaglio finale di un attacco, potrebbero comunque involontariamente costituire l'anello più debole della catena attraverso il quale i criminali informatici riescono ad accedere ai sistemi dell'impresa. Le piccole PMI potrebbero non essere il bersaglio ideale dell'attacco, ma potrebbero comunque apparire interessanti agli occhi dei criminali. Confidare eccessivamente nelle conoscenze di terzi potrebbe anche spostare il problema e la sua soluzioneal di fuori della sfera di responsabilità individuale, limitando ulteriormente la consapevolezza e la reattività in caso di attacco informatico.

2.7. PROATTIVO E IMPEGNATO

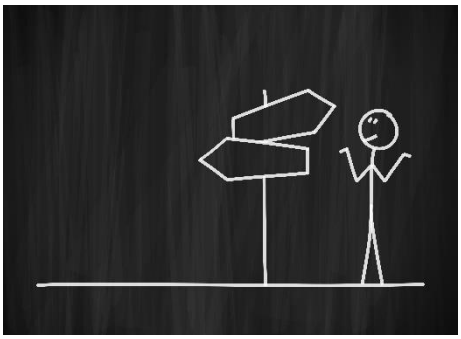
Parlando di potenziali attacchi e interruzioni di esercizio, gli intervistati hanno manifestato un'ampia gamma di reazioni. Anziché sentirsi paralizzati, si sono mostrati desiderosi di affrontare il problema e andare avanti. Una strada immersa nella nebbia –una situazione in cui si dispone di informazioni limitate – è diventata una metafora per trovare il percorso giusto nonostante le avversità, mentre un segnale stradale senza scritte è diventato il simbolo della necessità di sviluppare una soluzione. Per mantenere operativa un'impresa in caso di interruzione d'esercizio si possono utilizzare molteplici strumenti basati su tecnologie e workflow più datati..

Figura 20: Nebbia

NEBBIA

Durante gli attacchi informatici tutto appare confuso, ma io desidero continuare il mio percorso e trovare una soluzione. Non mi spaventa ciò che si cela nella nebbia, ma mi devo muovere con cautela per non smarrire la strada.

Figura 21: Pianificazione



PIANIFICAZIONE

Dovete scrivere i segnali voi stessi e non esiste una soluzione standard. I segnali puntano in direzioni diverse, perché si possono avere soluzioni differenti per lo stesso problema. Può darsi che dobbiate utilizzare il vostro cellulare personale se i sistemi dell'impresa non funzionano.

Figura 22: Come ai vecchi tempi

COME AI VECCHI TEMPI

Durante l'attacco al nostro fornitore, siamo ritornati a telefono, carta e penna, come ai vecchi tempi. Tutto ha funzionato abbastanza bene, fatta eccezione per le informazioni contabili che erano salvate nel sistema.

Questa mentalità proattiva e questo desiderio di andare avanti sono un asset importante per le PMI. Anziché aspettare il ripristino della normale attività da parte dei fornitori di servizi IT esterni, i dipendenti hanno voluto aiutare a mantenere operativa l'impresa. Con un po' di pianificazione e formazione, le PMI svizzere dovrebbero riuscire a sviluppare un workflow offline basato su cooperazione, energia e motivazione dei dipendenti. Questo dovrebbe evitare interruzioni improvvise e critiche delle loro interazioni con i clienti e aumentare la loro capacità di resistere a un attacco informatico.

Discussione

I dipendenti che abbiamo intervistato hanno manifestato un ventaglio di emozioni ampiamente variegato nel pensare e parlare di attacchi informatici. Non sorprende che queste diverse emozioni fossero discordanti, pur coesistendo nella mente dei soggetti. Queste emozioni possono essere raggruppate in sette temi principali che, in certa misura, si applicano a tutti gli intervistati. Ciascun tema è stato trattato separatamente nella Sezione 2. Alcuni punti possono essere ulteriormente differenziati sulla base di caratteristiche specifiche dei dipendenti e sono trattati nel paragrafo seguente. Inoltre, siamo anche riusciti a sviluppare raccomandazioni attuabili per le PMI e i loro fornitori di servizi.

3.1. IMPATTO PER CATEGORIA DI DIPENDENTI

Durante le interviste, abbiamo colto alcuni ulteriori segnali indicanti atteggiamenti differenti a seconda della categoria dei dipendenti. Sia le categorie sia le differenze sono puramente aneddotiche e sono il risultato delle nostre osservazioni, e non di nozioni teoriche o fondamentali. Ciononostante, riteniamo aggiungano valore alla nostra discussione.

3.1.1. Personale amministrativo vs. di produzione

La prima differenza osservata è stata tra i dipendenti amministrativi che svolgono lavoro d'ufficio e quelli impiegati nella produzione o presso le sedi dei clienti. Normalmente, i dipendenti del reparto produzione hanno accesso limitato ai sistemi IT – perlopiù collegati ai sistemi di produzione – e, in generale, si sentono quindi meno colpiti direttamente dagli attacchi informatici. Al contrario, i dipendenti amministrativi sono fortemente consapevoli delle conseguenze di tali problemi. Ricordano situazioni di indisponibilità dei sistemi per periodi prolungati o l'impatto dell'attacco a Meier Tobler sul loro lavoro. Di conseguenza, i dipendenti amministrativi dovrebbero essere propensi a sostenere lo sviluppo di processi di fallback e ad implementarli regolarmente.

3.1.2. Giovani vs. maturi

Un'altra differenza potenziale – e suggerita da numerosi intervistati – è quella tra dipendenti giovani e più maturi, laddove le persone più mature potrebbero essere più vulnerabili agli attacchi rispetto a quelle più giovani. I dipendenti più giovani avevano chiaramente maggiore familiarità con la tecnologia digitale ed erano più attivi sulle piattaforme dei social media. I dipendenti più maturi hanno affermato di non essere cresciuti con la tecnologia e di percepirla ancora come poco familiare. Di conseguenza, hanno dimostrato un approccio più cauto – potenzialmente più attenti a messaggi sospetti, più riluttanti a essere coinvolti e più disposti a chiedere consiglio quando insicuri, in particolare in un contesto lavorativo. Sebbene non sia possibile distinguere il profilo di rischio relativo effettivo, le risposte degli intervistati suggeriscono che tali differenze potrebbero non essere significative. I dipendenti più giovani hanno maggiore dimestichezza con la tecnologia e sono quindi più consapevoli dei rischi, tuttavia i dipendenti più maturi compensano tendenzialmente la loro mancanza di dimestichezza con una maggiore cautela.

3.1.3. Esperti vs. neofiti

Una potenziale classificazione analoga, seppur distinta, si basa sul livello di conoscenze digitali. Questo aspetto appare in certa misura correlato all'età, nonostante all'interno del gruppo dei più giovani siano risultate evidenti differenze significative nei livelli di conoscenze autodescritti. I dipendenti con maggiori conoscenze erano anche più sicuri della propria capacità di individuare gli attacchi informatici e di ritornare operativi. Inoltre, hanno mostrato la tendenza a considerare qualunque perdita come di piccola entità. I dipendenti con minori conoscenze si proteggono generalmente limitando la propria esposizione online e utilizzando solo piattaforme specifiche (ad es., e-banking) ove ritengono che un terzo fornisca un livello di sicurezza adeguato. Sebbene sia difficile definire il reale impatto di tali differenze, non è chiaro se una maggiore sicurezza di sé si traduca in una minore vulnerabilità

potenziale. I dipendenti che, a livello soggettivo, ritengono di avere maggiori conoscenze – e, quindi, si sentono più sicuri di sé – potrebbero assumere un comportamento meno avverso al rischio ed esporsi a maggiori pericoli.

3.1.4. Professionale vs. privato

Un'ulteriore differenza riguarda il comportamento individuale e sembra essere influenzata dal contesto (ad es., lavorare sul sistema e-mail della società o su un dispositivo personale). Gli intervistati hanno affermato di essere più prudenti in un contesto lavorativo, in parte sulla base delle interazioni esterne/con i clienti e in parte perché ritengono che il potenziale di danno sia maggiore. Inoltre, i contesti lavorativi sono tendenzialmente più complessi, con scambi che spesso contengono nomi di clienti e partner sconosciuti che richiedono quindi maggiore attenzione. Diversi dipendenti hanno riferito di e-mail fraudolente da clienti o fornitori falsi e la conseguente tendenza a un atteggiamento più difensivo. Le interviste hanno evidenziato un approccio meno attento in un contesto personale. Questo in parte perché i rispondenti ritenevano di riuscire a individuare più facilmente nomi o thread sospetti e perché la maggior parte degli intervistati non si considera sufficientemente importante da giustificare un attacco informatico. Questa distinzione potrebbe rappresentare una minaccia se questo atteggiamento più rilassato venisse trasferito in un contesto lavorativo o se i dispositivi personali fossero violati oppure utilizzati per compromettere i sistemi dell'impresa. La probabilità di questa minaccia aumenta ulteriormente quando ai dipendenti viene regolarmente richiesto di lavorare da casa, come ad esempio nel caso dell'attuale pandemia da coronavirus.

3.2. RACCOMANDAZIONI PER IL MIGLIORAMENTO

Le nostre raccomandazioni per il miglioramento si basano su alcune osservazioni inequivocabili ricavate dalle interviste. In linea generale, i dipendenti sono motivati e proattivi; tuttavia, considerano spesso gli attacchi informatici come un problema per esperti. Gli esperti sono di fatto necessari, tuttavia ognuno può contribuire a sviluppare soluzioni e a ripristinare l'operatività in seguito a un attacco. Inoltre, non è chiaro in quale misura i dipendenti siano consapevoli del rischio e delle potenziali conseguenze per la loro organizzazione. In considerazione di ciò, raccomandiamo tre aree chiave di miglioramento. Questi miglioramenti possono essere realizzati autonomamente dalle imprese oppure offerti da fornitori esterni nell'ambito dei loro servizi. Queste raccomandazioni sono complementari alla consulenza standard per le imprese e sono finalizzate a rendere sicura la loro infrastruttura e a mitigare la gravità dei potenziali attacchi. L'infrastruttura dovrebbe essere rafforzata con firewall adeguati, misure di sicurezza fisica e basata su password, nonché attraverso la messa a punto di una risposta d'emergenza e un piano di ripristino. La gravità di un attacco può essere controllata individuando e proteggendo gli asset più preziosi dell'impresa, i cosiddetti «gioielli della corona». Questi sono spesso dati proprietari, informazioni sui clienti e attrezzature di produzione. Le raccomandazioni tratte da questo studio sono concepite per potenziare queste indicazioni generali, in particolare nel caso delle PMI.

3.2.1. Aumentare la consapevolezza

I dipendenti sembrano essere consapevoli sia delle conseguenze potenzialmente catastrofiche degli attacchi informatici, sia della propria vulnerabilità, in particolare verso i tentativi di phishing. Al contempo, considerano la loro impresa troppo insignificante per giustificare un attacco. Gli attacchi informatici vengono inoltre considerati parte di una lotta politica globale anziché un'insidia vicina alla propria realtà. Naturalmente, questo atteggiamento è rischioso e vi sono statistiche nazionali e numerosi casi celebri che servono da monito. Queste informazioni devono essere comunicate ai dipendenti in modo diretto e sistematico. Inoltre, i dipendenti dovrebbero essere informati regolarmente in merito al numero di attacchi falliti all'infrastruttura IT dell'impresa, ricordando loro al contempo quali misure si stanno adottando (ad es. upgrade dei firewall) per proteggersi. Occorre anche ricordare loro le semplici abitudini da adottare per ridurre il rischio. Le imprese dovrebbero anche testare le proprie difese di sistema e vulnerabilità umane, magari utilizzando hacker etici – se possono permettersi l'esborso – dato che i dipendenti vedono di buon occhio gli hacker che lavorano per il bene comune. I risultati dovrebbero essere quindi comunicati ai dipendenti per dare risalto all'importanza del loro ruolo nella salvaguardia dell'impresa.

3.2.2. Responsabilizzare i dipendenti

Esiste la diffusa convinzione che gli hacker siano soggetti particolarmente esperti e ben equipaggiati, che il mondo informatico sia complesso e che i fornitori di servizi specializzati rappresentino la principale linea di difesa. Sebbene

questo possa essere in certa misura vero e i fornitori di servizi professionali rappresentino parte di una protezione efficace e di un sistema di risposta, non possono agire in modo isolato. L'esternalizzazione della responsabilità relativa alla sicurezza informatica a terzi induce a un approccio più lassista da parte dei dipendenti, il cui comportamento online rappresenta una linea di difesa vitale contro gli attacchi. Inoltre, i dipendenti delle PMI sono tendenzialmente proattivi e desiderano partecipare alle misure di contrasto. Oltre ad aumentare la consapevolezza del loro ruolo, i dipendenti dovrebbero essere incoraggiati a partecipare all'individuazione e alla comunicazione degli attacchi ed essere coinvolti nello sviluppo di soluzioni (vedere il paragrafo 3.2.3 di seguito). Sarebbe opportuno chiedere ai fornitori di servizi esterni di istruire i dipendenti e di coinvolgerli il più possibile.

3.2.3. Esercitarsi a lavorare in modalità di ripristino

In caso di attacco, o più comunemente, un malfunzionamento del sistema, i dipendenti potrebbero non sapere come comportarsi. Le loro reazioni non dovrebbero essere però improvvisate o ad hoc. Tali scenari dovrebbero essere pianificati in anticipo, fornendo strumenti di supporto e definendo chiaramente i fattori di attivazione delle procedure di emergenza. Le nostre interviste hanno indicato che, in particolare, è difficile accedere alle informazioni di fatturazione dei clienti e alle specifiche tecniche di prodotto quando si lavora offline e questo punto deve essere affrontato attentamente.

Lo sviluppo di uno scenario non IT può anche rappresentare un'opportunità per stimolare lo spirito di collaborazione e far leva sulle conoscenze di ciascun dipendente. A titolo esemplificativo, le società possono proporre un workshop in cui i dipendenti cercano di svolgere il proprio lavoro quotidiano senza i normali strumenti IT. In questo modo, scopriranno presto quali informazioni sono vitali e devono essere rese disponibili mediante sistemi offline, quali compiti possono essere svolti sui dispositivi personali e quali devono essere su base cartacea. Questi strumenti possono essere in seguito sviluppati durante la normale attività lavorativa e testati periodicamente mediante esercizi «live fire» quando l'attività si svolge senza l'infrastruttura IT standard. L'attività lavorativa in modalità di ripristino dovrebbe disporre di trigger esatti e predefiniti in funzione del sistema colpito e della durata dell'interruzione.

Figura 23: Raccomandazioni per il miglioramento

RACCOMANDAZIONI PER IL MIGLIORAMENTO

PREPARARSI

AUMENTARE LA CONSAPEVOLEZZA

RESPONSABILIZZARE I DIPENDENTI

ESERCITARSI A LAVORARE IN MODALITÀ DI RIPRISTINO

Conclusioni

Gli attacchi informatici rappresentano un problema importante e in progressivo aumento, e le PMI svizzere non sono escluse da questa evoluzione. Gli ultimi anni hanno fatto registrare una crescita degli attacchi ransomware mirati o di altre minacce finanziarie e anche attacchi malware più generali hanno colpito le PMI svizzere. Oltre a un'infrastruttura tecnologica ben progettata e aggiornata, la consapevolezza dei dipendenti e un comportamento online attento sono componenti cruciali di qualunque meccanismo di difesa, in quanto gli attacchi informatici iniziano normalmente con l'infiltrazione nei sistemi IT attraverso attacchi di phishing. Questi attacchi sfruttano le debolezze umane per ottenere password e altre informazioni cruciali. L'attività di phishing viene svolta in modo pressoché ininterrotto e spesso possono trascorrere diversi mesi tra un tentativo di phishing riuscito e l'attacco vero e proprio, fatto che rende difficile il tracciamento e il feedback per i dipendenti. Il livello «normale» di consapevolezza e di comportamento online dei dipendenti è pertanto l'indicatore più significativo della vulnerabilità agli attacchi di phishing.

Per questo studio, abbiamo intervistato diversi dipendenti di tre PMI svizzere al fine di comprendere le loro opinioni sugli attacchi informatici. La nostra ricerca si è basata su metafore profonde per comprendere i fattori emotivi e nascosti del comportamento dei dipendenti di fronte alla minaccia rappresentata dal crimine informatico. Le risposte sono state aggregate in temi comuni che evidenziano l'ampia varietà di emozioni e pensieri associati al mondo digitale. I dipendenti hanno collocato gli attacchi informatici nel contesto più generale della politica globale, riconoscendo al contempo i motivi di carattere puramente economico e criminale da cui scaturisce al maggior parte degli attacchi. Considerano gli hacker operatori qualificati e ben attrezzati, ma non sempre come una forza negativa. Si sentono vulnerabili e impotenti di fronte agli attacchi informatici e riconoscono il danno potenziale che questi eventi possono causare. Al contempo, considerano la loro impresa e se stessi tendenzialmente troppo piccoli per essere bersaglio di un attacco e, in questa eventualità, fanno affidamento su esperti esterni per ricevere protezione. Tuttavia, sono fondamentalmente proattivi e interessati a lavorare per trovare soluzioni pratiche.

Abbiamo presentato tre suggerimenti attuabili per le PMI svizzere per migliorare le raccomandazioni generali esistenti per la sicurezza informatica. Questi suggerimenti fanno leva sugli elementi positivi della cultura prevalente delle PMI e affrontano gli aspetti più rischiosi. È necessaria una maggiore attività informativa per aumentare la consapevolezza, così come strumenti adeguati, per agevolare il passaggio verso una padronanza più diretta da parte dei dipendenti dei problemi e delle relative soluzioni. Inoltre, le società devono mettere a punto un piano di emergenza e organizzare esercitazioni operative che permettano loro di prepararsi all'eventualità di un breakdown del sistema. Nell'ambito di ulteriori indagini sarebbe opportuno valutare se esistono differenze tra i dipendenti che rispondono agli attacchi di phishing e quelli che non lo fanno, se i dipendenti di grandi organizzazioni hanno atteggiamenti analoghi nei confronti della sicurezza informatica e se le misure che suggeriamo in questa sede sono in grado di mitigare la minaccia rappresentata dagli attacchi informatici.

Bibliografia

Allianz (2020). *Allianz Risk Barometer 2020*. (accesso eseguito il 25 novembre 2020) https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-it.html

Anz P. (2020). *Daten aus Cyber-Attacke auf Stadler Rail veröffentlicht*. (accesso eseguito il 25 novembre 2020) https://www.inside-it.ch/de/post/daten-aus-cyber-attacke-auf-stadler-rail-veroeffentlicht-20200529

Borkert S. (2020). *Bankrott auch mit Cyberangriff begründet: Wurde Mörschwiler Swisswindows in den Ruin gehackt?*. (accesso eseguito il 25 novembre 2020) https://www.tagblatt.ch/wirtschaft/bankrott-auch-mit-cyberangriff-begruendet-wurde-moerschwiler-swisswindows-in-den-ruin-gehackt-ld.1198956

Christensen G.L. e Olson J.C. (2002). Mapping Consumers' Mental Models with ZMET. *Psychology and Marketing*, vol. 19 (6): 477-502. doi: 10.1002/mar.10021

Damasio A. R. (1994). Time-locked multiregional retroactivation: A systems level proposal for the neural substrates of recall and recognition. In P. D. Eimas & A. Galaburda (Eds.), *Neurobiology of cognition* (pp. 24–62). Cambridge, MA: MIT Press.

de Moura G. et al. (2020). *Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal*. World Economic Forum (accesso eseguito il 25 novembre 2020) https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal

Dreissigacker A., von Skarczinski B. e Wollinger G.R. (2020).*Cyberangriffe gegen Unternehmen in Deutschland*. Kriminologisches Forschungsinstitut Niedersachsen e.V., Forschungsbericht 152

Ufficio federale di statistica (2020). *Cifre sulle PMI*. (accesso eseguito il 25 novembre 2020) https://www.kmu.admin.ch/kmu/it/home/fatti-e-tendenze/politica-pmi-fatti-e-cifre/cifre-sulle-pmi/aziende-e-lavoro.html

Griesser Kym T. (2020). *Nach Cyberangriff: Erpresser erhöhen Druck auf Stadler*. Tagblatt. (accesso eseguito il 25 novembre 2020) https://www.tagblatt.ch/wirtschaft/erpresser-erhoehen-druck-auf-stadler-ld.1235844

Heer A. (2020). *Ecco come i criminali informatici attaccano le aziende*. (acceso eseguito il 25 novembre 2020) https://www.swisscom.ch/it/magazine/sicurezza-dati-infrastrutture/cyber-attacchi-azienda-malware-phishing/

Jochum K. (2019). *Offix von massivem Hacker-Angriff getroffen*. (accesso eseguito il 25 novembre 2020) https://www.inside-it.ch/de/post/offix-von-massivem-hacker-angriff-getroffen-20190703

Klein R. (2020). *Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite*. (accesso eseguito il 25 novembre 2020) https://dataloft.ch/security/schweizer-fensterfirma-swisswindows-ag-geht-nach-ransomware-angriff-pleite/

Lüscher A., e Niedermann M. (2019). *Hacker legen Schweizer Grossunternehmen lahm*. SRF (accesso eseguito il 25 novembre 2020) https://www.srf.ch/news/wirtschaft/geht-es-um-loesegeld-hacker-legen-schweizer-grossunternehmen-lahm

Luzerner Zeitung (2019). *Cyberattacke gegen Meier Tobler legt Betrieb weitgehend lahm*. (accesso eseguito il 25 novembre 2020) https://www.luzernerzeitung.ch/wirtschaft/cyberattacke-gegen-meier-tobler-legt-betrieb-weitgehend-lahm-ld.1138900

Mändli Lerch K. e Repic, A. (2017). *Cyberrisiken in Schweizer KMUs*. (accesso eseguito il 25 novembre 2020) https://gfs-zh.ch/wp-content/uploads/2017/12/Schlussbericht_CyberriskKMU_12122017.pdf

Meier Tobler (2020). *Geschäftsbericht 2019 Meier Tobler Group AG*. (accesso eseguito il 25 novembre 2020) https://www.meiertobler.ch/de/content/download-file/6534/file/25.02.20%20Gesch%C3%A4ftsbericht%202019.pdf

MELANI (2020a). *Attenzione: i rischi di sicurezza per le PMI causati da ransomware continuano a essere elevati*. (accesso eseguito il 25 novembre 2020) https://www.ncsc.admin.ch/ncsc/it/home/aktuell/news/bollettino-d-informazione/sicherheitsrisiko-durch-ransomware.html

MELANI (2020b). *Rapporto semestrale 2020/1*. (accesso eseguito il 25 novembre 2020) https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte/rapporti-di-situazione/rapporto-semestrale-2020-1.html

Moser S. (2019). Cyberrisiken – die unterschätzte Gefahr. *Neue Zürcher Zeitung*. 22 maggio 2019.

Olson J. C. e Reynolds, T. J. (1983). Understanding consumers' cognitive structures: Implications for advertising strategy. In L. Percy & A. G. Woodside (Eds.), *Advertising and consumer psychology* (pp. 77–90). Lexington, MA: Lexington Books.

Papedis (n. d.). *OFFIX Holding AG*. (accesso eseguito il 25 novembre 2020) https://www.papedis.ch/it/azienda/gruppo-offix/.

Pugnetti C. e Bekaert X. (2018). *A Tale of Self-Doubt and Distrust. Onboarding Millennials: Understanding the Experience of New Insurance Customers*. ZHAW School of Management and Law, ISBN 978-3-03870-021-0.

Pugnetti C. e Schneebeli M. (2020). Kundenbedürfnisse und Marktpenetration. Schweizer KMUs unterschätzen die Bedeutung von Dienstleistungen und Versicherungsdeckungen gegen Cyberrisiken. *Schweizer Versicherung*, gennaio 2020.

Pugnetti C., Casián C., Staub N. e Ellenberger T. (2019). Cyber-Resilienz steigern. *Schweizer Versicherung*, ottobre 2019.

Schäppi M. (2020). *Cyberattacke auf Meier Tobler, Dienstleister der Gesundheitsbranche*. (accesso eseguito il 25 novembre 2020) https://www.infosec-health.ch/_Resources/Persistent/77d3731325caf3cb4a5060a02fea716d543be3c3/K_Ref2_Sch%C3%A4ppi_Cyberangriff%20auf%20DL%20der%20Gesundheitsb.pdf

Severin C. (2019). *Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat*. (accesso eseguito il 25 novembre 2020) https://www.offix.ch/media/cms/Offix/Media/NZZ_Cyber-Angriff%20auf%20KMU_OFFIX-Gruppe.pdf

SIA (2018). *Grundlagenpapier des SVV zu Cyber-Risiken*. Gruppo di lavoro Cyber-Risk, Associazione Svizzera d'Assicurazioni (accesso eseguito il 25 novembre 2020) https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf

SRF (2020). *Offenbar zwang eine Cyberattacke Swisswindows in die Knie*. (accesso eseguito il 25 novembre 2020) https://www.srf.ch/news/regional/ostschweiz/konkurs-fensterhersteller-offenbar-zwang-eine-cyberattacke-swisswindows-in-die-knie

Stadler Rail (2020a). *Geschäftsbericht 2019*. (accesso eseguito il 25 novembre 2020) https://www.stadlerrail.com/media/pdf/web_stadler_rail_gb19_de.pdf

Stadler Rail (2020b). *Cyber-attack against Stadler IT network*. (accesso eseguito il 25 novembre 2020) https://www.stadlerrail.com/media/pdf/2020_0507_media%20release_cyber-attack_en.pdf

Trustwave (2020). *2020 Trustwave Global Security Report*. (accesso eseguito il 25 novembre 2020) https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/

Zaltman G. (1997). Rethinking Marketing Research: Putting People Back In. *Journal of Marketing Research*, Vol. 34, 4. https://doi.org/10.1177/002224379703400402.

Zaltman G. e Zaltman L. (2008). *Marketing Metaphoria: What Deep Metaphors Reveal about the Minds of Consumers*. Harvard Business Press.

Tabelle

Figure

Autori

Il Dr. Carlo Pugnetti è docente presso l'Istituto Risk & Insurance della ZHAW. La sua ricerca è dedicata all'evoluzione del comportamento del cliente in ambito assicurativo, e si concentra in particolare sui cambiamenti innescati dall'adozione della tecnologia e dalle differenze generazionali. Pugnetti svolge anche ricerche sul legame tra innovazione e gestione dei rischi.

Prima di entrare alla ZHAW, Carlo Pugnetti ha rivestito la carica di CEO presso Allianz Global Assistance in Svizzera e numerose altre funzioni nel Gruppo Allianz – nell'ambito delle quali si è occupato della ristrutturazione dei Sinistri di Fireman's Fund negli Stati Uniti, di aspetti strategici nell'ambito del Gruppo a Monaco di Baviera e della direzione di un ramo di attività internazionale a Parigi. Carlo Pugnetti ha iniziato la sua carriera come consulente per Oliver Wyman.

Ha conseguito un dottorato in Analisi di Rischio e un master in Ingegneria Elettronica, entrambi alla Stanford University.

Carlos Casián è underwriter in ambito Property and Cyber Risk presso Allianz Suisse. Ha condotto programmi di formazione interni ed esterni e partecipato a numerosi panel di esperti. Carlos Casián è oratore pubblico per Allianz nell'ambito dei rischi informatici e rappresenta Allianz Suisse nel Gruppo di lavoro Cyber Risk dell'Associazione svizzera d'Assicurazioni.

Carlos Casián ha acquisito ampie conoscenze in ambito assicurativo partendo da zero, iniziando la sua carriera in Allianz Suisse oltre dieci anni fa. Negli ultimi anni, ha concentrato la propria attenzione sui rischi informatici e sul loro impatto sui profili di rischio delle imprese.

Carlos Casián ha conseguito un Bachelor of Science (BSc) in Economia aziendale con una specializzazione su rischio e assicurazione presso la ZHAW.

Partner

I nostri più sinceri ringraziamenti alle nostre aziende partner che hanno messo a disposizione i propri dipendenti e sostenuto questo studio.

Kurt Wyss, partner
VTL Insurance + Partner AG

www.vtl.ch

Sokol Prendi, Head of Sales
Dätwyler Fertigungs-Technologie AG

www.daetwylerag.ch

Manuel Fischer, CEO
Fischer Wärmetechnik AG

www.heizprofi.ch

Terence Iseli, CEO
ISELI ENERGIE AG

www.iseli-energie.ch

Xavier Bekaert, Partner
Benthurst & Co.

www.benthurst.com

School of Management and Law

St.-Georgen-Platz 2
Casella postale
8401 Winterthur
Svizzera

www.zhaw.ch/sml

AACSB ACCREDITED

swissuniversities