Cyber-rischi, coperture, servizi e sinistri

Mara Jardini, Senior Underwriter AXA

Webinar ASG, 05.03.2024

Agenda

60 Min.

1. Cyber-rischi	Perché può essere interessata ogni azienda? Perché può essere interessato ogni gestore patrimoniale esterno? Sondaggi, statistiche
2. Quali coperture assicurative esistono ?	
3. Servizi	
4. Sinistri	Esempio di sinistro
5. Domande e discussione	


1
Cyber-rischi

1.1 Perche ogni azienta può essere interessata

Obiettivo aziendale: Sicurezza delle informazioni

La cyber-sicurezza va intesa come gestione dei rischi a livello aziendale
Ogni problema rilevante in materia di sicurezza IT viene teoricamente risolto, e ciononostante possono risultare catastrofi!

Proprietà Intellettuale

Vantaggio Competitivo

Protezione dei dati
Fiducia del cliente

Certezza giuridica
Responsabilità della direzione

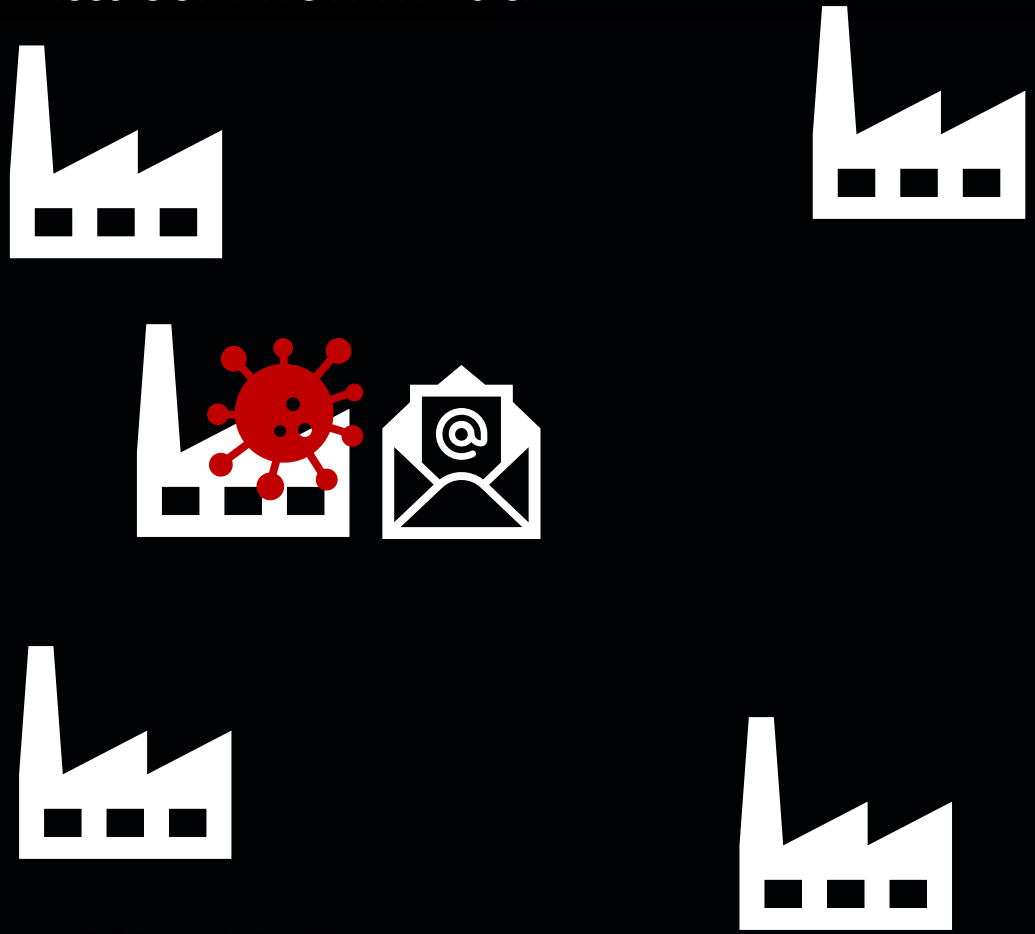
Prevenzione dei danni
Riduzione dei costi

Sicurezza delle forniture
Disponibilità della merce

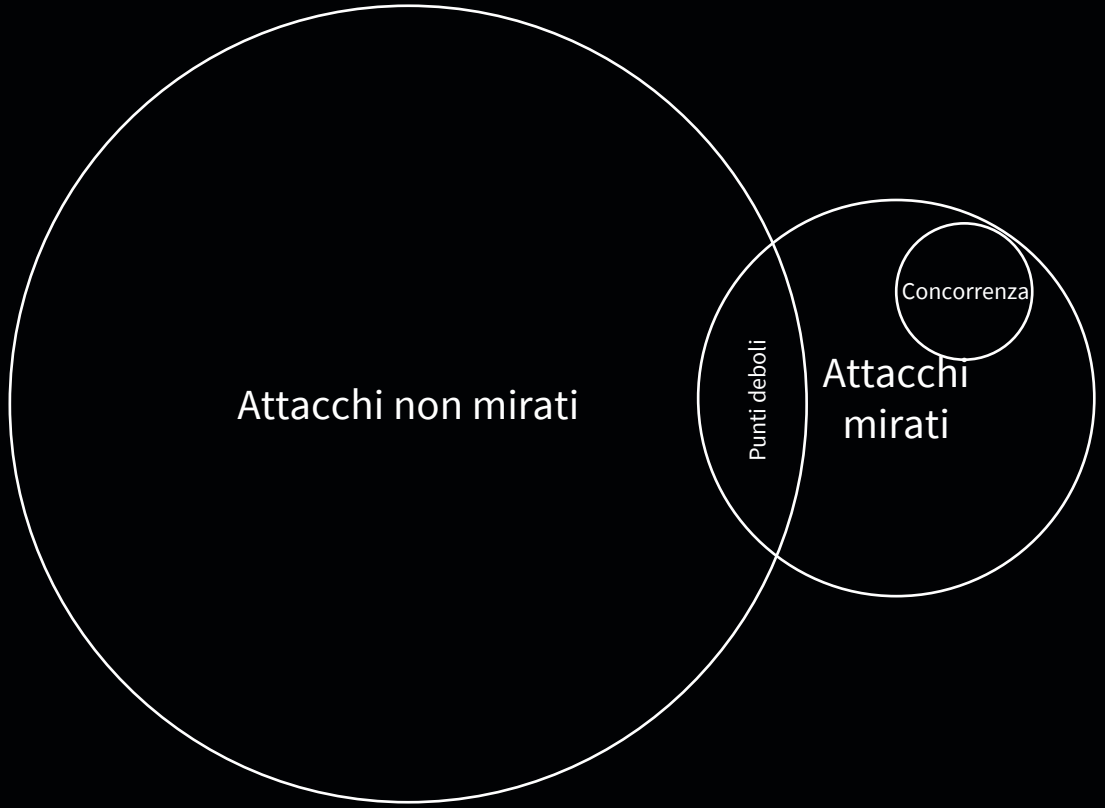
Determinazione
Obbiettivo di Rischio

Attacchi mirati

Attacchi non mirati



Attacchi non mirati



Le persone al centro

Raccomandazioni del' UFCS (ex-NCSC)

del 29 Gennaio 2024 (rapporto Anti-Phishing 2023, in parte abbreviato)

- **Notifica all'UFCS:** Segnalare e-mail o siti web sospetti all' UFCS: antiphishing.ch.
- **Siate scettici:** nessuna banca o istituto di carte di credito vi chiederà mai via email o SMS di cambiare la password of di verificare i dati della vostra carta di credito.
- **Autentificazione a più fattori (MFA):** ove possibile, attivate sui vostri account online, ad esempio e-mail o social media, un'autenticazione a più fattori (MFA).
- **Utilizzo ripetuto di password:** non usare mai la stessa password per più die un conto online. Utilizzate un password manager per gestire i vostri dati di accesso
- **Conteggio della carta di credito:** verificate regolarmente se vi sono inesattezze nel conteggio mensile della carta di credito. In caso transazioni sconosciute rivolgetevi subito alla società della carta di credito..
- **Utilizzo dei favoriti:** per l'accesso regolare ai conti online come ad esempio e-banking, social media o e-mail utilizzate la funzione Preferiti («Bookmarks») del vostro web browser.
- **Spoofing:** Ricordate che i mittenti di e-mail e SMS, ma anche i numeri di telefono delle chiamate in entrata possono essere facilmente falsificati. Nel dubbio esigete di poter richiamare la persona che chiama.

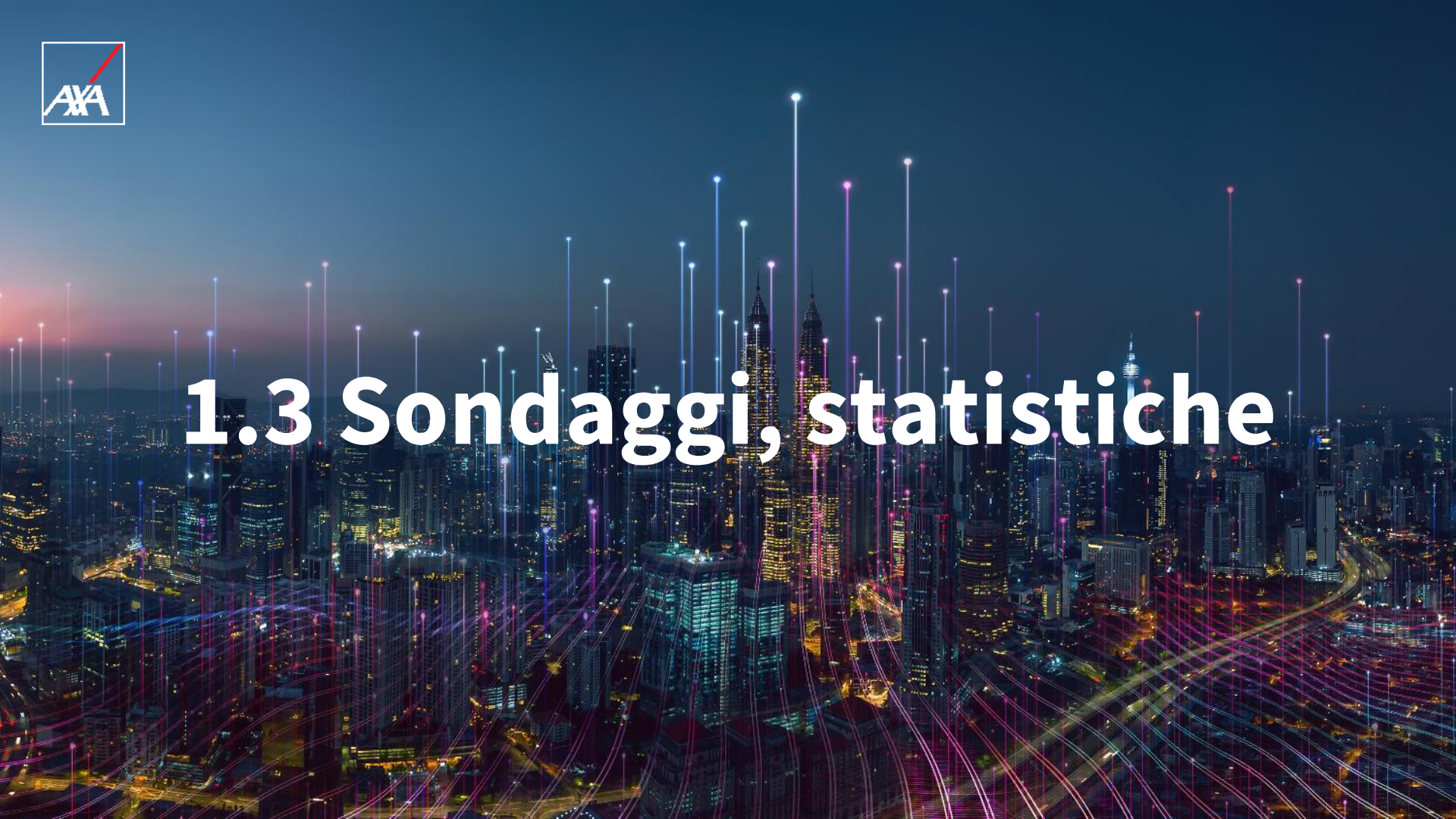

1.2 Perchè ogni gestore patrimoniale dovrebbe essere interessato?

Gestori patrimoniali e cyber-sicurezza

- IT & cyber-sicurezza
  - giudicato dalla stragrande maggioranza dei gestori patrimoniali esterni in Svizzera come molto importante e necessita d'intervento nell'arco di 12 mesi - tre anni
  - Il ramo che affida l'IT e la cyber-sicurezza in maggior parte a numero di fornitori esterni di servizi (circa il 60%)
    - Fonte: Status Quo der Digitalisierung und internen Organisation der externen Vermögensverwalter, Studio di Tatiana Agnesens, Luzern, Gennaio 2024
- Cybercriminalità nella gestione patrimoniale
  - I gestori patrimoniali hanno spesso accesso diretto al patrimonio die clienti. I criminali cercano di approfittare di questa situazione
  - Basta un clic per installare un malware in grado di dare accesso all'e-banking e inducono il collaboratore a effettuare pagamenti non motivate (frode del CEO)
  - I cyber-criminali si spacciano spesso per un membro della direzione e possono indurre collaboratori a effettuare pagamenti fraudolenti(frode del CEO)
  - I collaboratori non hanno ricevuto una formazione sufficiente su come riconoscere il phishing (contenuti internet falsificati
    - Fonte: Newsletter VSV-ASG di Andreas Corradini (AXA), Dicembre 2022

Gestori patrimoniali nella stampa

- «Un noto gestore patrimoniale svizzero hackerato– i dati rubati ritrovati nel darknet» (Watson.ch titolo del 7.02.2023)
  - I cyber-criminali sono riusciti a penetrare nei server di Finaport AG e a sottrarre grandi quantità di dati. Si parla di 1.2 terabytes.
  - La Finaport ha confermato che i dati rubati dai server sono stati pubblicati nel darknet
  - Entro 24 ore Finaport ha provveduto a informare le autorità
  - Erano presenti die backup di tutti i dati interessati
  - I cyber-attacchi continueranno a moltiplicarsi. La quantità, qualità e complessità sono in forte aumento
  - L'obbligo di notifica delle autorità di vigilanza nei confronti della FINMA è uno strumento importante per l'individuazione di cyber-attacchi
  - Secondo la stampa Finaport AG non è risultata indenne. Alte informazioni non sono disponibili al pubblico



1.3 Sondaggi, statistiche

Studio Cyber AXA e statistiche della polizia criminale

15% delle imprese vittime di un attacco cyber nel 2021

14 % delle piu piccole PMI

29 % delle grandi PMI

Un’azienda su

10

È stata ripetutamente attaccata

33’345

Reati nel settore della criminalià digitale nel 2022

+10%

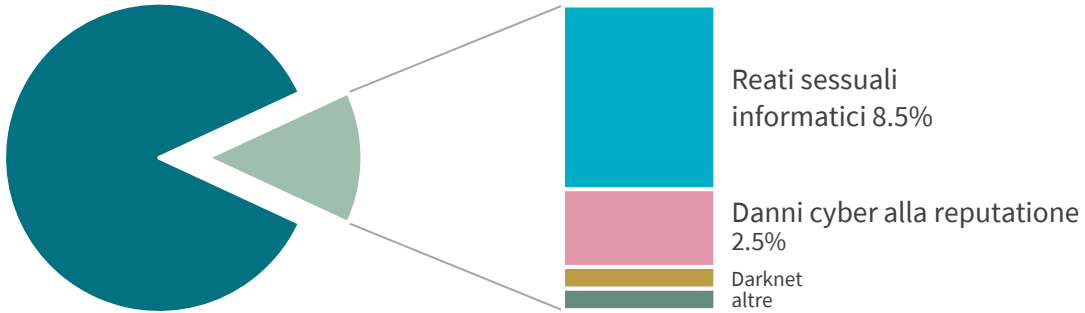
Aumento dal 2021 al 2022

Fonti: Studio AXA CH, agosto 2022, statistiche della polizia criminale 2022, 2023

Cybercriminalità (criminalità digitale)

Nel 2022 sono stati registrati 33’345 reati con una componente digitale (+10% rispetto al 2021)
La quota dei casi risolti è del 34.3%

Settori della criminalità digitale



Cybercriminalità economica 89.0% (29677 reati), ad es. Abuso die sistemi di pagamento, truffa del CEO, truffa digitale

Fonte: statistiche della polizia criminale, rapporto annuale 2022, Neuchâtel, 2023

Cybercriminalità (criminalità digitale)

Quali sono stati nel 2022 i reati più frequenti della cybercriminalità economica ?

- Phishing: 2’236
- Hacking: Introduzione con la forza in un sistema informatico 246
- Hacking: Intrusione un sistema di elaborazione dati con accesso di dati di terzi 796
- Malware –Ransomware 307
- Malware –E-Banking 49
- Malware –Spyware 15
- Malware –Rogueware/Scareware 45

Fonte : statistiche della polizia criminale, rapporto annuale 2022, Neuchâtel 2023

«Il rischio esiste, ma non riguarda la mia azienda»

Una credenza errata e pericolosa

Gli intervistati che vedono solo un rischio esiguo per la propria azienda dicono…

60%
la mia azienda è troppo piccola

81%
i nostri sistemi informatici sono protetti a 360°

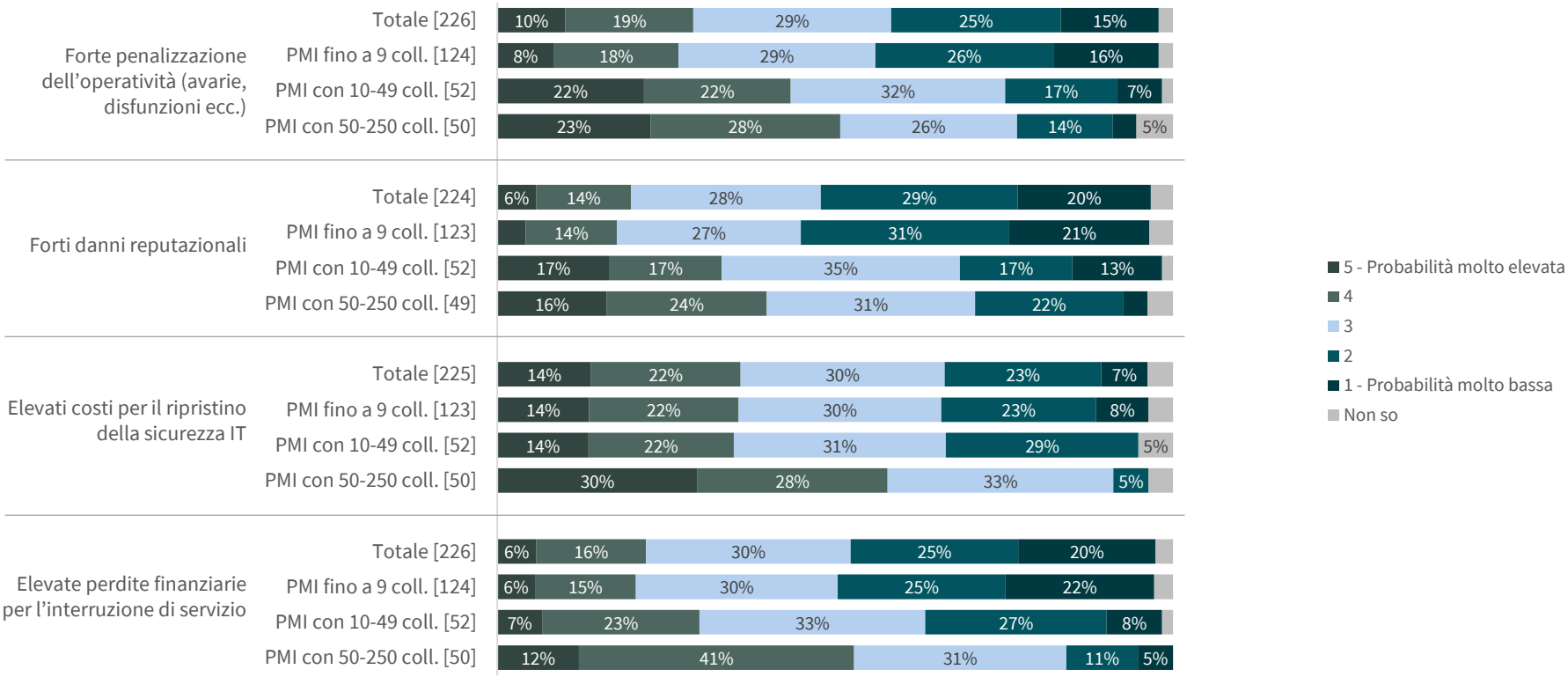
58%
non siamo mai stati vittima di un cyberattacco

70%
i nostri dati non sono interessanti

Fonte: Cybersecurity for SMES, Challenges and Recommendations, ENISA, giugno 2021

Studio AXA Cyber Security

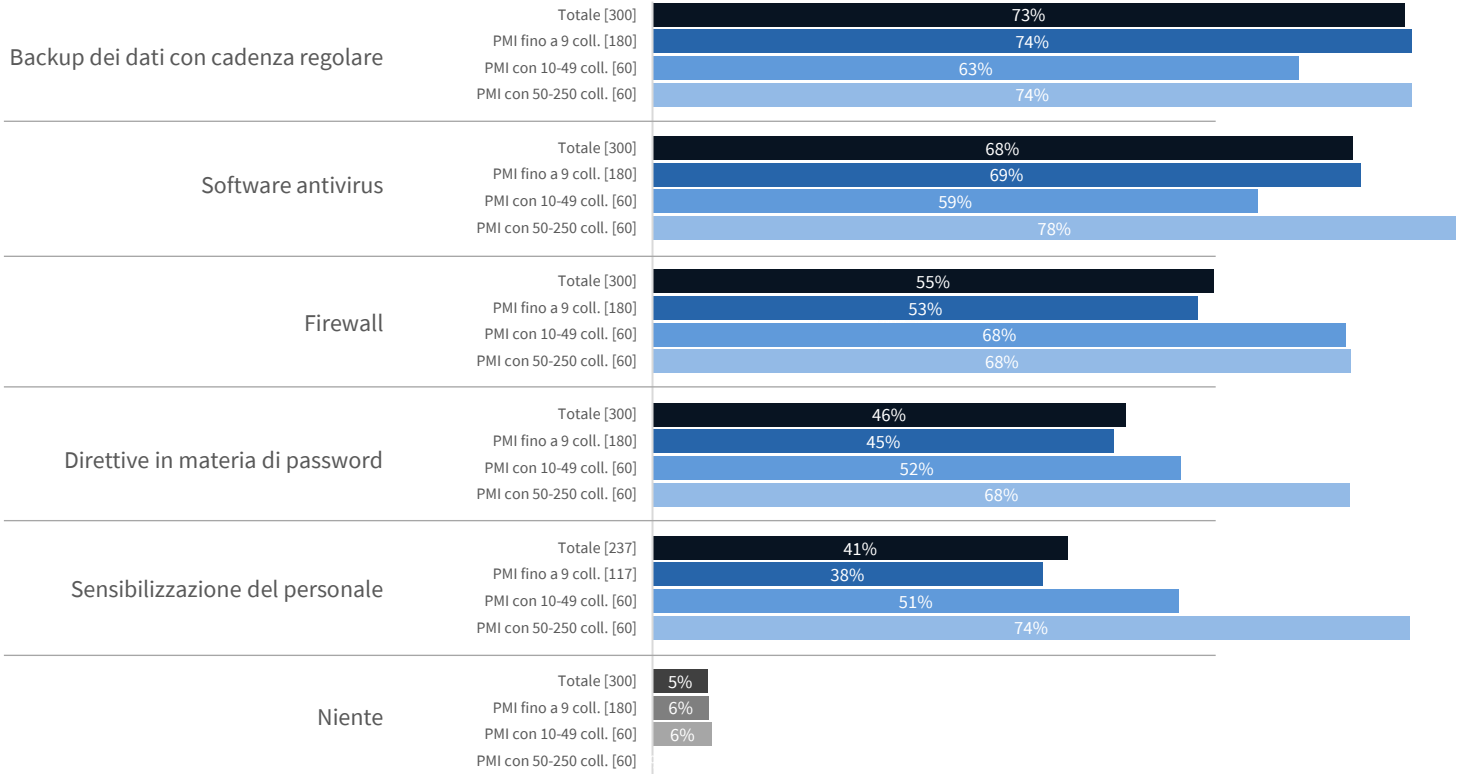
Quali conseguenze si prevedono?



Fonte: Studio AXA CH, agosto 2022

Studio AXA Cyber Security

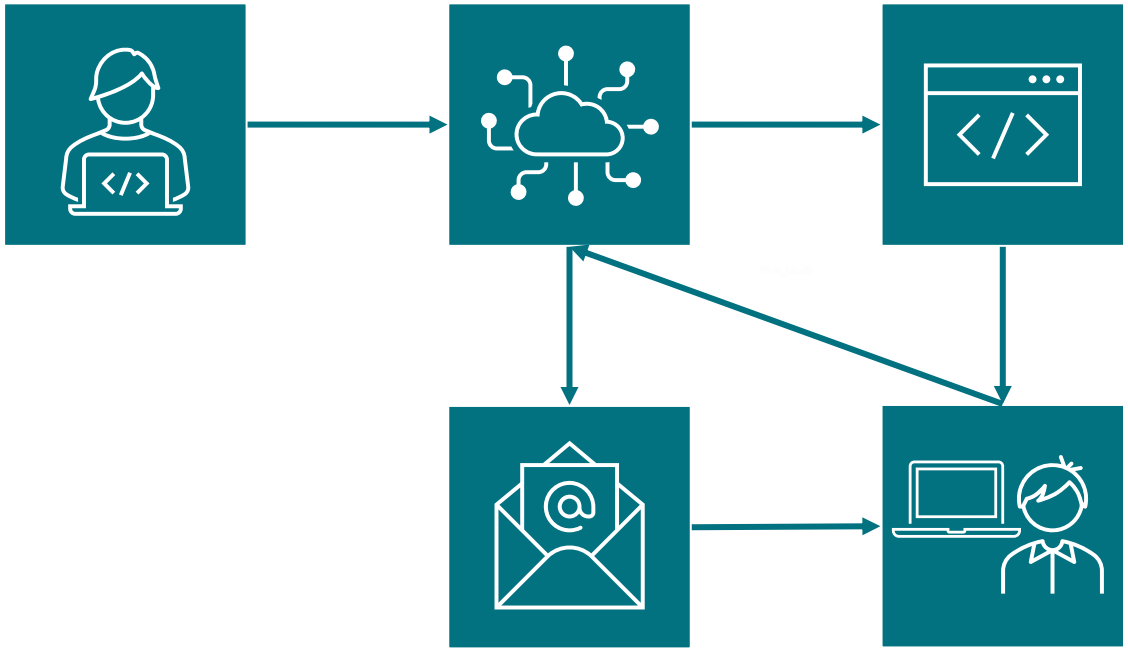
Misure adottate dalle aziende



Fonte: Studio AXA CH, agosto 2022


2
Quali coperture assicurative esistono?

Le basi – Cyber-evento

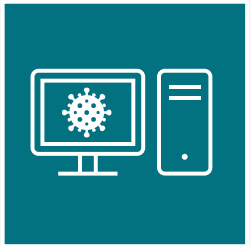
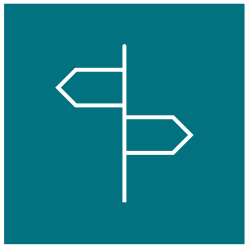


«… un attacco intenzionale e nocivo…»

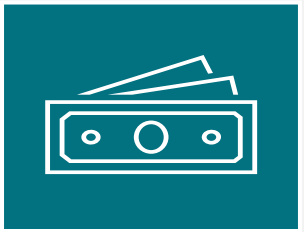
«… al *sistema IT dello stipulante* o ai *sistemi di cloud computing*…»

CGA E2-E4

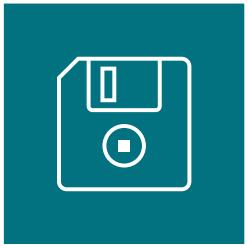
Le basi – Coperture

Cyber-evento con danni propri	Cyber-evento con danno RC	Assistenza in caso di crisi	Coperture addizionali
			 Online banking  Hacking telefonico  Social engineering  Richiesta di riscatto
• Spese di ripristino • Interruzione d'esercizio • Violazione delle norme sulla protezione dei dati	• Risarcimento di pretese giustificate • Difesa contro le pretese ingiustificate	• Misure immediate • Consulenza per la gestione della crisi • Comunicazione in caso di crisi	
CGA B1	CGA B2	CGA B3	CGA B4-B6

Le basi – Coperture addizionali

Manipolazione E – banking, del webshop o dell'invio di merci	Hackeraggio telefonoci	Social Engineering	Richiesta di riscatto
			
• Pagamenti non autorizzati dell'e-banking • Furto di denaro di terzi • Manipolazione della manipolazione di merci • Danno proprio e RC	• Utilizzo dell impanto telefonico da parte di terzi dopo un cyber-evento con danno proprio	• Frodo • Presa di contatto personale del truffatore • Sfruttamento della buona fede	• Inkl. Spese per le trattative
AVB B4	AVB B5	AVB B6	AVB C1.12

Basi – Obblighi



Backup

- Almeno ogni 7 giorni (offline)
- Test di ripristino raccomandato (non nelle CGA)

Sistemi di sicurezza

- Antivirus
- Firewall ecc.

Aggiornamenti

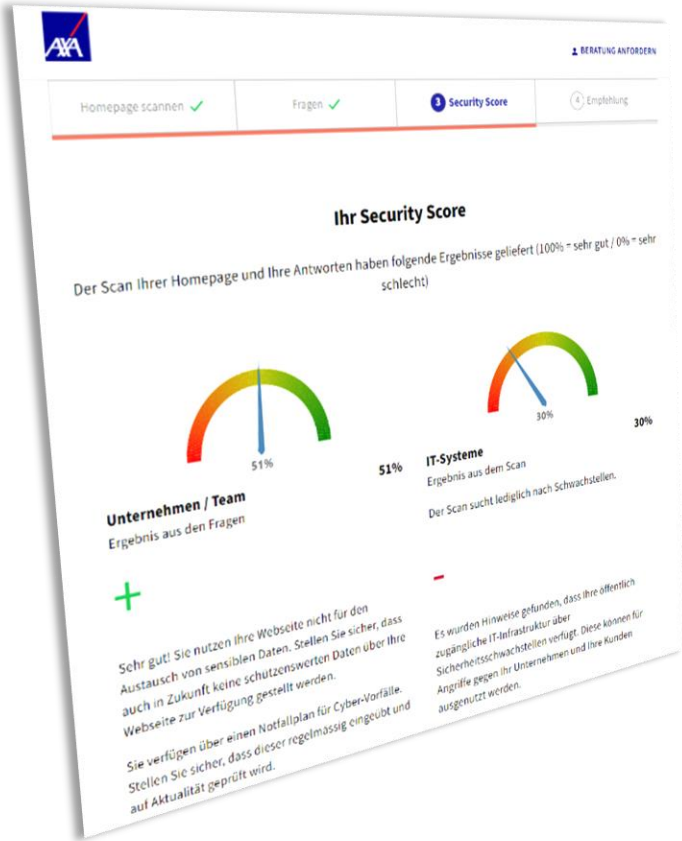
- Sistemi operativi, di sicurezza e di altro tipo
- A breve scadenza

«… misure richieste dalle circostanze per proteggere i *dati* assicurati contro i rischi coperti dall'assicurazione…»

CGA A11

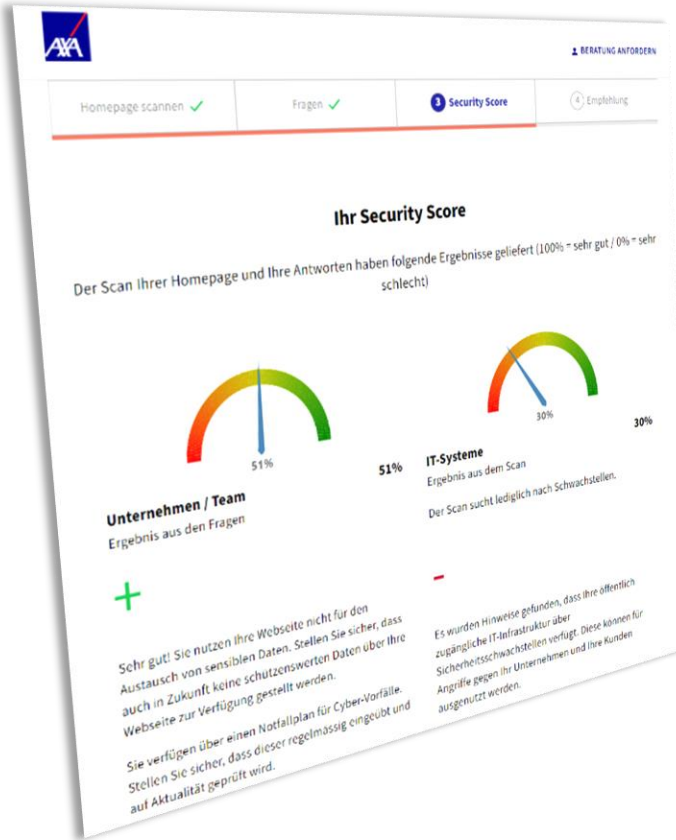

3
Servizi

Cyber-Check e protezione



Servizio di prevenzione de cyber-risch

Cyber-Check e protezione



cyber-check.axa.ch

- ✓ Breve autotest per PMI sulle tematiche della sicurezza informatica
- ✓ «Apri-porta»
- ✓ Creazione di consapevolezza
- ✓ Scansione della homepage tramite vulnerability test

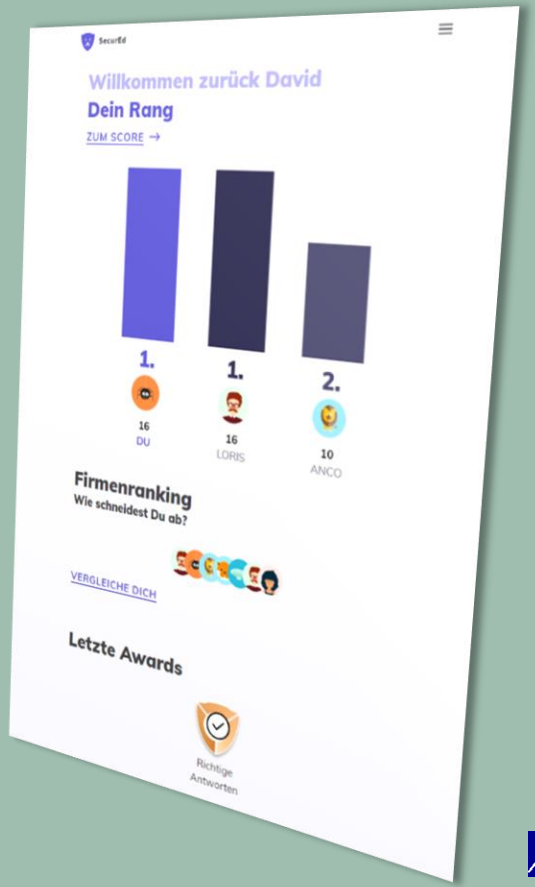
- ✓ **Novità – Offerte possibili tramite calcolatore PMI**

Servizio di prevenzione dei cyber-rischi

www.scrd.ch

- ✓ Piattaforma di formazione per il personale
- ✓ Gamification per maggiore motivazione
- ✓ Blog sulla sicurezza informatica con lacune attuali
- ✓ Vulnerability scan – Facciata esterna infrastruttura

- ✓ **Gratis per ogni cliente Cyber**
- ✓ Registrazione su www.axa.ch/cps



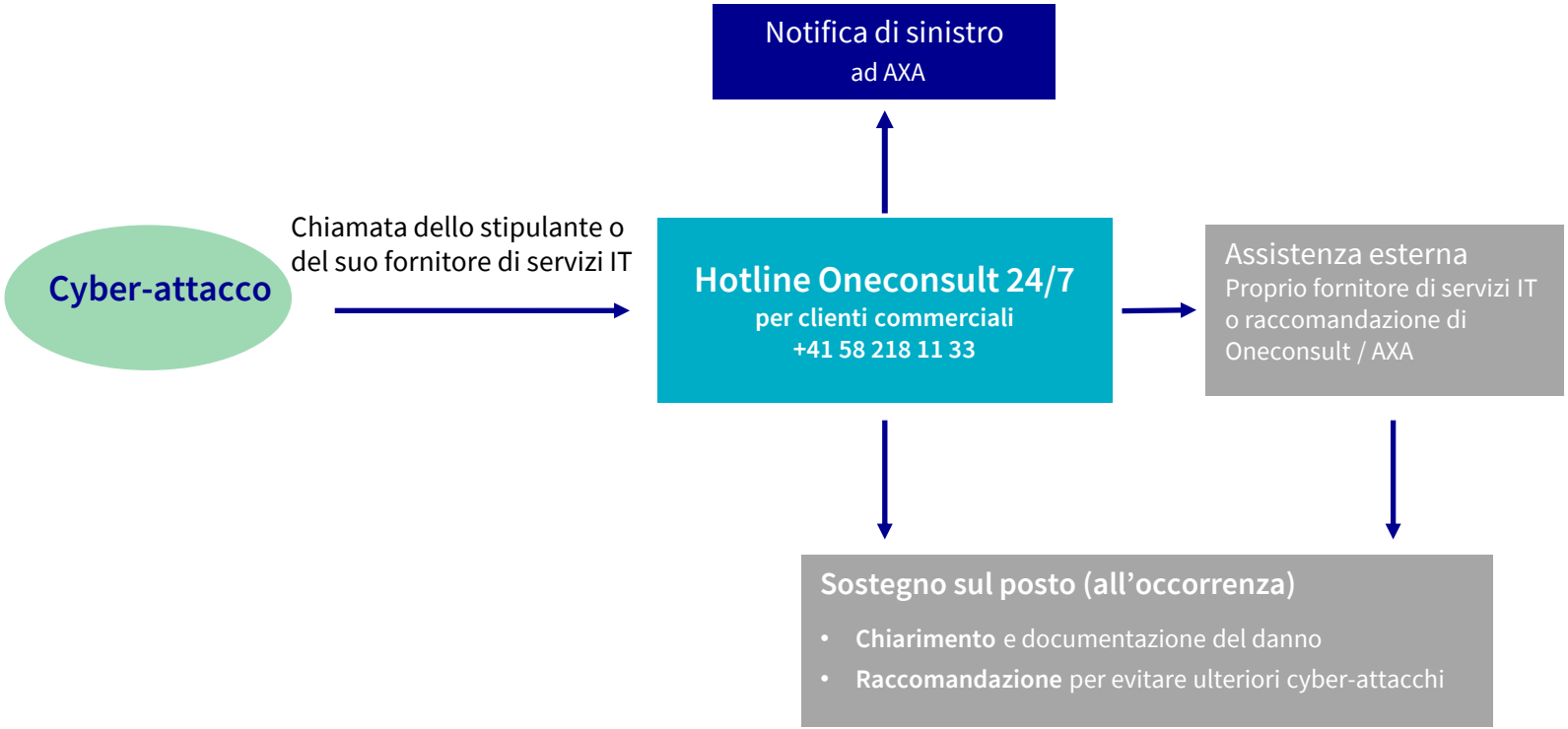

4
Sinistri

Le tre linee di difesa

L’assicurazione cyber è la terza linea di difesa

Il processo di notifica di sinistro

Comportamento in caso di sinistro per clienti commerciali



Assistenza immediata in caso di sinistri cyber

Tramite Oneconsult AG

- Stima di un esperto della situazione illustrata
- Raccomandazione di misure immediate per limitare i danni
- Raccomandazione di misure immediate per determinare le cause
- Prima valutazione delle misure già adottate

- Le spese per l'assistenza immediata non sono soggette a franchigia e non vengono dedotte dalla somma assicurata
- Ciò vale anche qualora dovesse risultare che il sinistro non è coperto
- L'assistenza immediata è limitata a un importo massimo di CHF 5'000. In questo lasso di tempo Oneconsult dovrebbe poter valutare se sussiste un evento assicurato


Esempio di sinistro
Rossi e Bernasconi

Introduzione Rossi e Bernasconi

Rossi e Bernasconi
Gestione Patrimoniale

- Gestione patrimoniale
- 5 collaboratori con postazione di lavoro
- Ciffra d’affari di CHF 780’000
- La copertura di base dell’assicurazione cyber è stata stipulata di recente

Sinistro Rossi e Bernasconi

Fase 1 BEC (Business Email Compromise)

Da: Nicole Rossi
A: Gaetano

Ciao Gaetano, potresti fare un versamento internazionale ? Fammi sapere, così posso inviarti i dati bancari e la fattura.

Cari saluti
Nicole Rossi
CEO

Da: Gaetano
A: Nicole Rossi

Certamente. Spediscimi pure la fattura.

Gaetano

Da: Nicole Rossi
A: Gaetano

Gaetano,

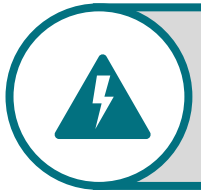
Per favore spediscimi la conferma del pagamento.

Cari saluti
Nicole Rossi
CEO

Esempio di sinistro Rossi e Bernasconi

Phase 1 BEC

- A seguito di un’email falsa, l’uffico contabile è stato invitato a effettuare un pagamento internazionale



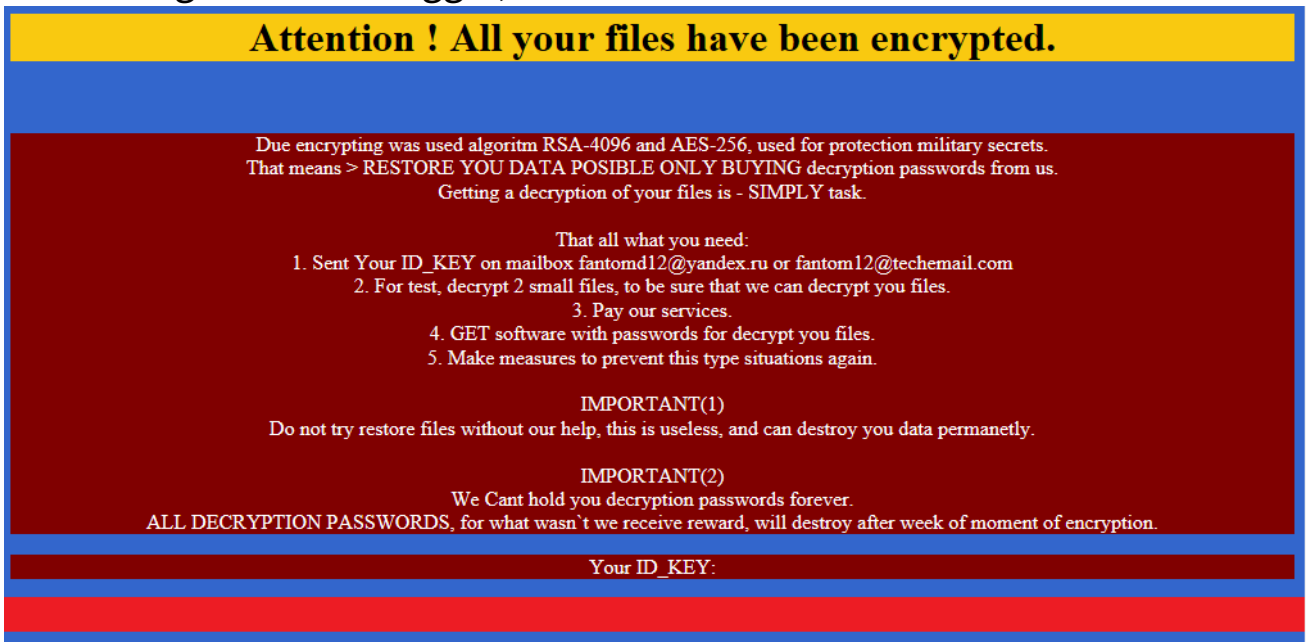
- Pagamento di EUR 25’000 al cyber-criminale
- Inoltre è stato installato e successivamente attivato un malware

- La copertura per pagamento errato è stata rifutata poichè il social engineering non è stato stipulato

Esempio di sinistro Rossi e Bernasconi

Fase 2 Ransomeware

Lunedi mattina, quando il signor Bianchi di Rossi e Bernasconi avvia il computer, sullo schermo viene visualizzato il seguente messaggio;



Esempio di sinistro Rossi e Bernasconi

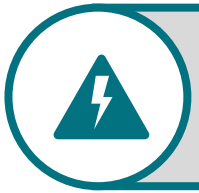
Fase 2 Ransomware
istruzioni dettaglate degli hacker

```
                                --> ATTENTION <--
DO NOT:
        Modify, rename, copy or move any files or you
        can DAMAGE them and decryption will be impossible
        Use any third-party or public Decryption software, it also may DAMAGE
files
        Shutdown or Reset your system, it can DAMAGE files
        Hire any third-party negotiators (recovery/police and etc)

        Your security perimeter was BREACHED
        Critically important servers and hosts were completely ENCRYPTED
        This README-FILE here for you to show you our presence
        in your's network and avoid any silence about hacking and leakage
        Also, we has DOWNLOADED your most SENSITIVE Data just in case if you
will NOT PAY,
        than everything will be PUBLISHED in Media and/or SOLD to any
third-party

1) WHAT SHOULD YOU DO:
        You have to contact us as soon as possible (you can find contacts below)
        You should purchase our decryption tool, so will be able to restore your
files
        Without our Decryption keys it's impossible
        You should make a Deal with us, to avoid your Data leakage

2) YOUR OPTIONS:
        IF NO CONTACT OR DEAL MADE IN 3 DAYS:
        Decryption key will be deleted permanently and recovery will be
impossible
        All your Data will be Published and/or Sold to any third-parties
        Information regarding vulnerabilities of your network also can be
published and/or shared

        IF WE MAKE A DEAL:
        We will provide you with the Decryption Key and Manual how-to-use
        We will remove all your files from our file-storage with proof of
Deletion
        We guarantee to avoid sharing any details with third-parties
        We will provide you the penetration report and list of
security-recommendations

                        Instructions for contacting our team

        Download and install TOR browser: https://torproject.org
        For contact us via LIVE CHAT open our
        > Website:
4jhwbypqhnbw4ee2gbbhpzlksybuvljbnvnzns2zkyp2t6urmkmq77qd.onion
        > Password: 4b34bc6d4700b411bb3ed468fe76817d
        If Tor is restricted in your area, use VPN
        All your Data will be published in 3 Days if NO contact made
        Your Decryption keys will be permanently destroyed in 3 Days if no
contact made
        Your Data will be published if you will hire third-party negotiators to
contact us
```

Esempio di sinistro Rossi e Bernascono

Phase 2 Ransomware

- Infezione di un singlo «Client» cliccando su un link
- Malware non è stato notato



- Criptaggio del server
- I «clients» sono stati in maggioranza criptati
- Richesta di riscatto in Bitcoin

✓ Backup regolari sono disponibili
× Il backup locale non è utilizzabile
✓ Il backup fuori sede (e «offline») era intatto

Conclusioni: esempio di sinistro Rossi e Bernasconi

Indennizzo	
Analisi dell'incidente, verifica del sistema	CHF 1'440.00
Ripristino die Sistemi	CHF 7'560.00
Miglioramenti vari apportati dopo la ricostituzione dei dati	CHF 2'880.00
Costi esterni	
OneConsult: Aiuto immediato Oneconsult	CHF 600.00
Indennizzo totale	**CHF 12'480.00**


5
Domande e discussione

Vantaggi AXA

Perchè AXA è il partner giusto per assicurazioni e servizi cyber

In casi sospetti, il reparto IT della PMI o il suo prestatario esterno dispone di interlocutori specializzati 24 ore su 24, 7 giorni su 7

Il servizio di prevenzione è gratuito per clienti con un polizza Cyber.

L'assistenza immediata è gratuita per i clienti, anche se non si verifica nessun sinistri coperto.

Gestione di Crisi grazie ad un sistema collaudato
Rete di esperti (incl. Copertura per spese di PR)

I soci dell' ASG usufruiscono di un ribasso del 10% sull'assicurazione cyber:
Link al calcolatore online ➔ Calcolatore PMI | AXA

Per ulteriori domande e osservazioni si prega di inviare una e-mail al nostro team specializzato:

AXA Assicurazione AG

Servizio specialistico assicurazioni

cyber clienti commerciali

cyber.security@axa.ch

Offerte esclusive per aziende aderenti all'ASG | AXA

Grazie per l’attenzione