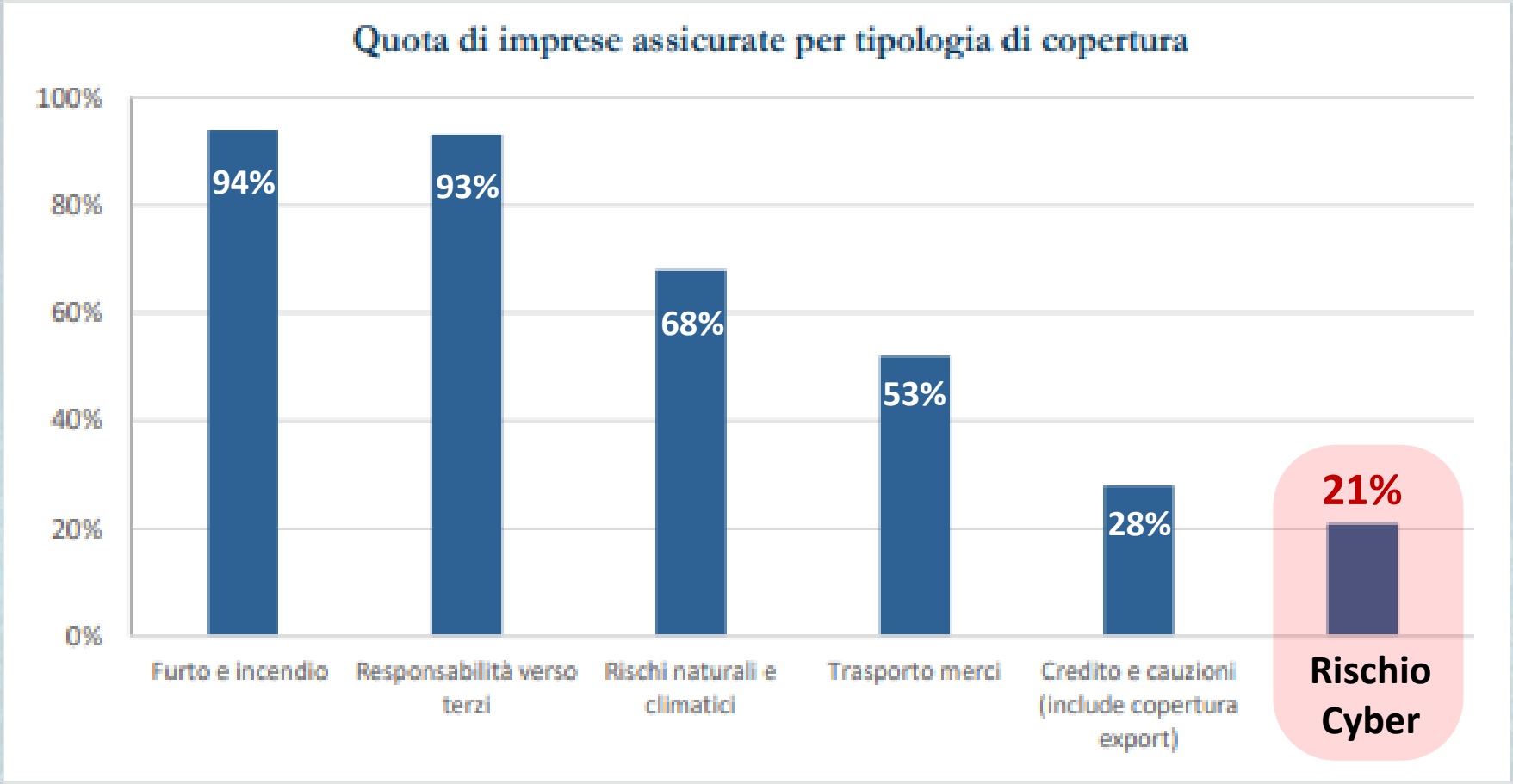

riCONOSCI le vulnerabilità
Come e dove indicarle alle PMI

BANCA D'ITALIA
EUROSISTEMA

Rischio cyber, la sottoassicurazione è molto forte per le imprese (21%)



Fonte - Indagine Bankitalia: PMI italiane sottoassicurate
6 Luglio 2022

Il rischio Cyber ha raggiunto le prime posizioni nell'elenco dei rischi globali per le PMI

358%[1]

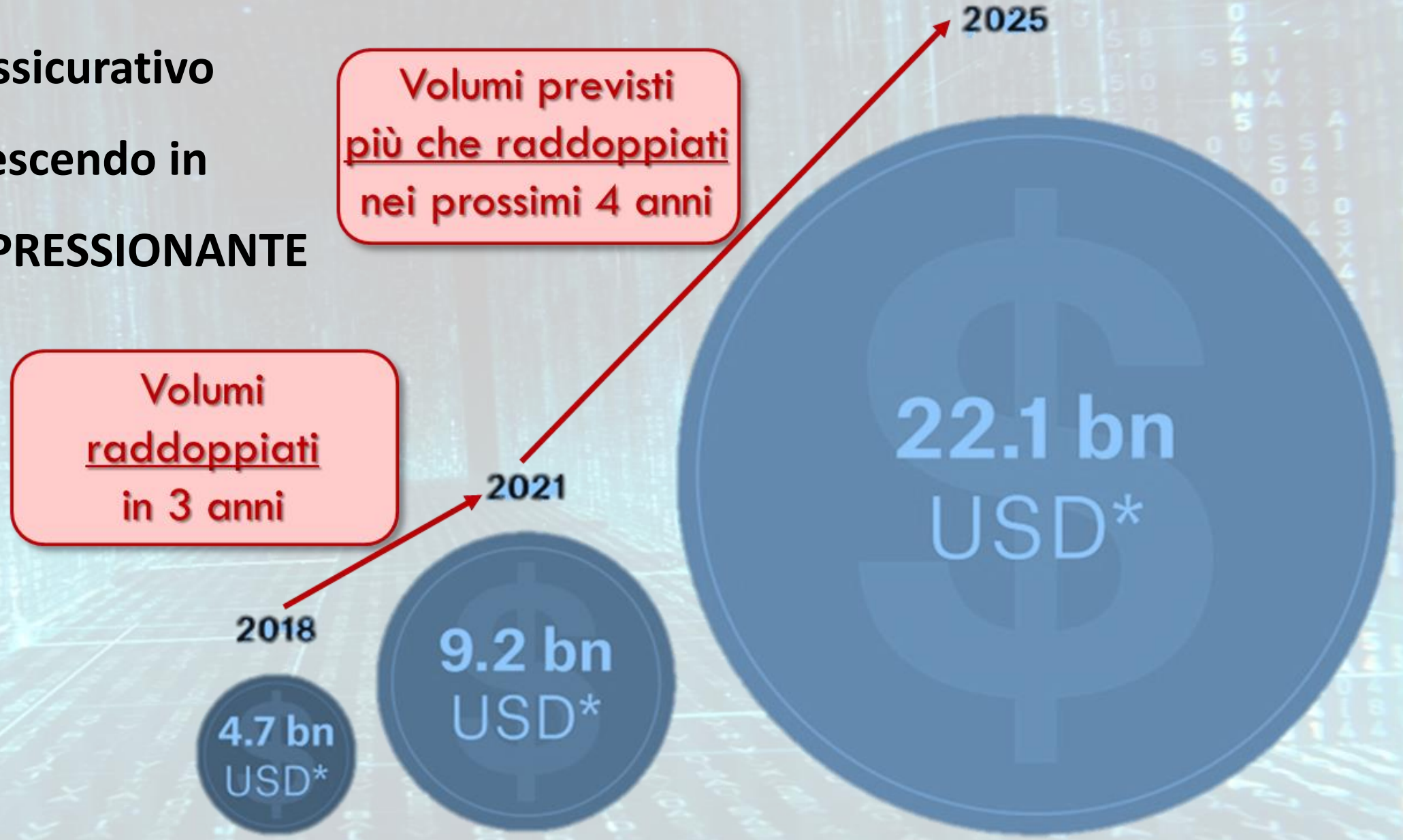
Incremento attacchi malware nel 2020

435%[1]

Incremento attacchi ransomware nel 2020

1. World Economic Forum (WEF) – Global Risk Report 2022

Il mercato assicurativo cyber sta crescendo in maniera IMPRESSIONANTE

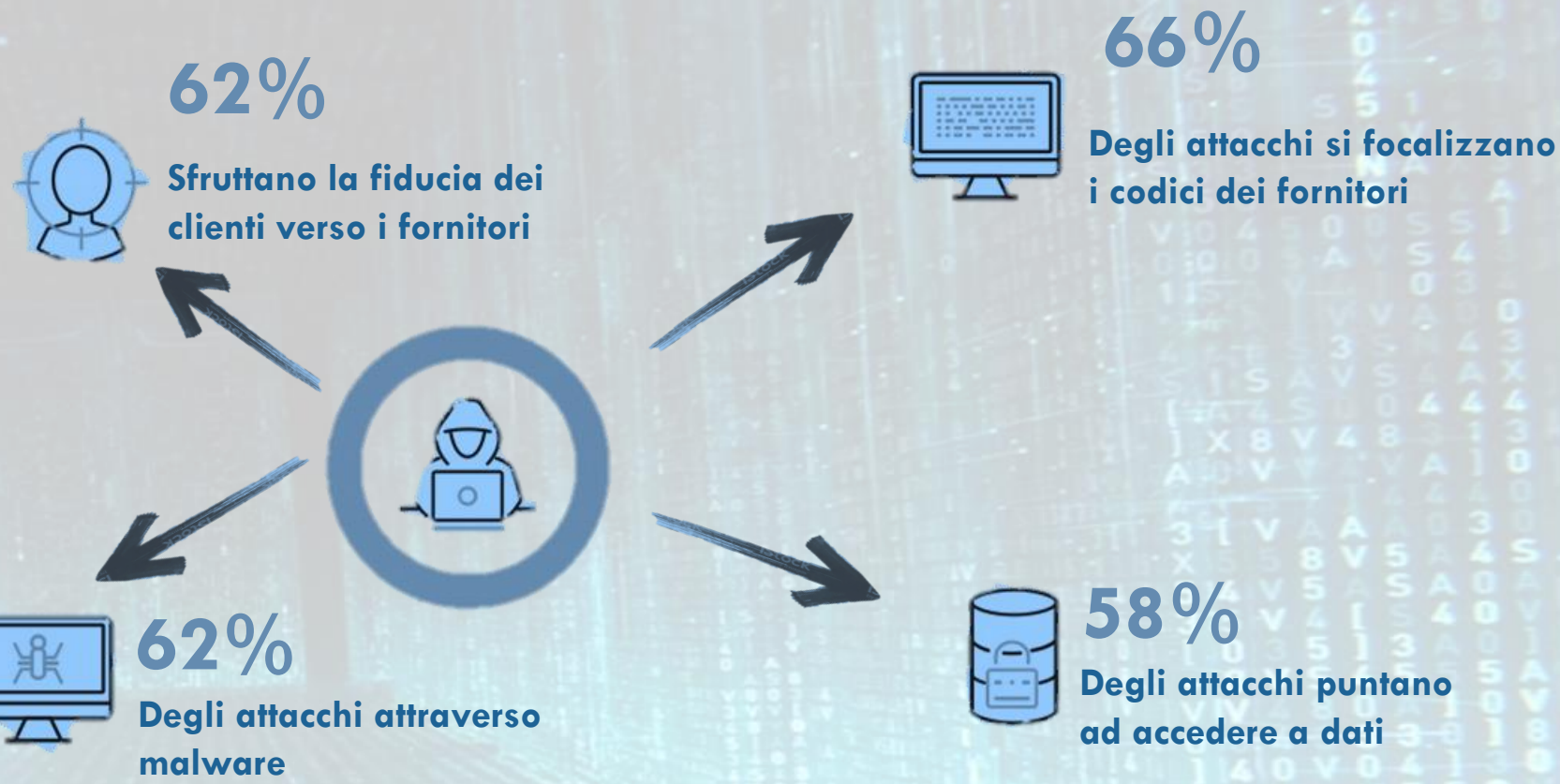


Fonte: Munich Re 2022

L’83% dei top manager affermano che la loro azienda non è adeguatamente protetta dalle minacce cyber

Fonte: Munich Re 2022

Gli attacchi cyber alla supply chain (catena di fornitori) sono in aumento



Fonte: Munich Re 2022

Una catena è forte quanto il suo anello più debole

A proposito di vulnerabilità ...

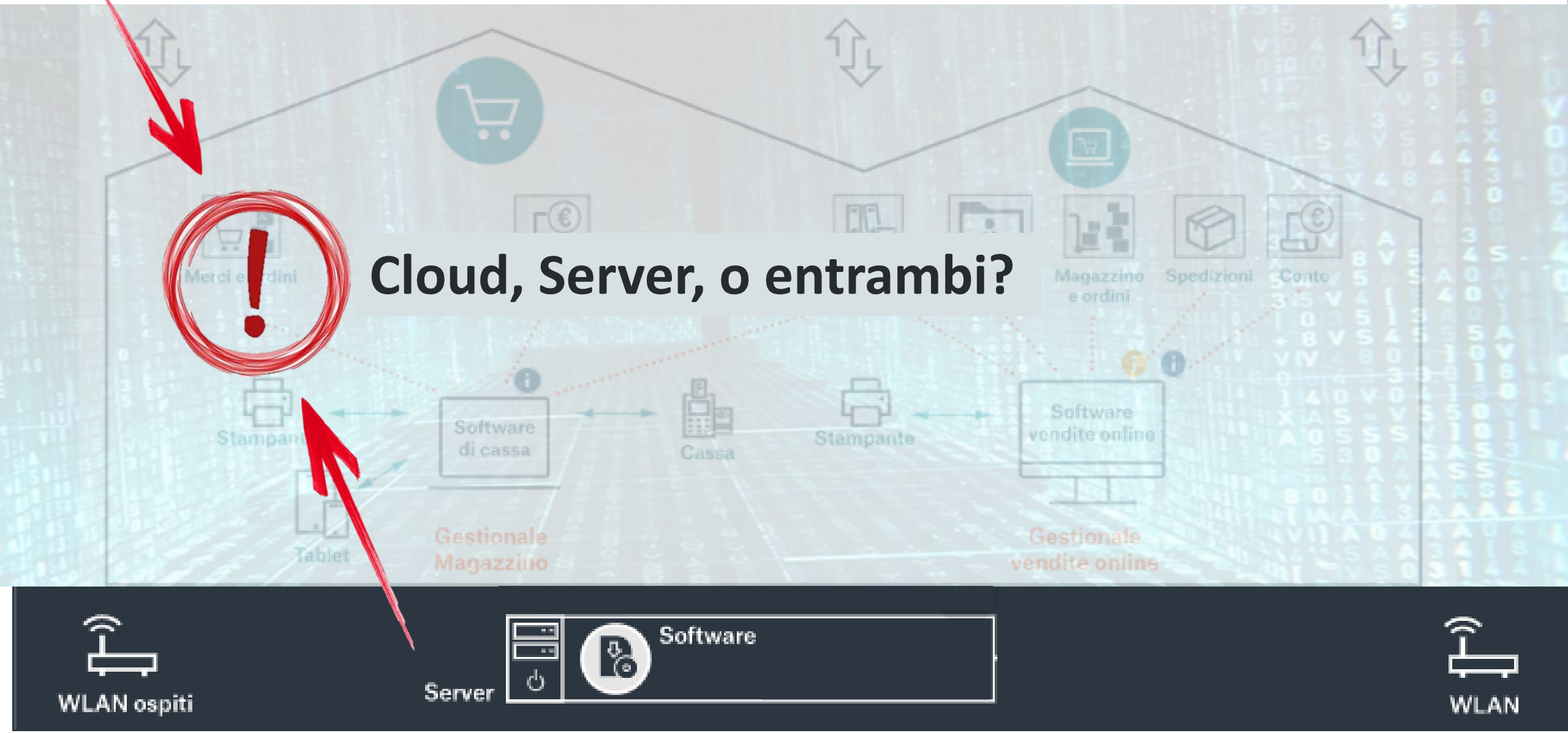
... Impariamo a riconoscere le **PORTE DI ACCESSO**

e **TESORI** nell'impronta digitale di una PMI

Porte di accesso

Obiettivi dell'infrastruttura IT che, se oggetto di attacco hacker, causerebbero il danno maggiore alla PMI

Cloud, Server, o entrambi?




Cloud
Mail
WEB
Internet
Fornitore
In linea
Portali
Valutazione del negozio
Fornitori
Fornitore di servizi
Provider IT
Fornitore servizi di pagamento
Cassa malattia
Banca
Conto
Contabilità
Gestionale clienti
Magazzino e ordini
Spedizioni
Conto
Software di cassa
Cassa
Stampante
Software vendite online
Tablet
Gestionale Magazzino
WLAN ospiti
Server
Software
WLAN


Cloud
Mail
WEB
Internet
Fornitore
In linea
Portali
Valutazi
negozio
Fornitori
di beni
Fornitori di servizi
Fornitori IT
Fornitore servizi
di pagamento
attia
Banca
Merci e ordini
Conto
Contabilità
Gestionale
clienti
Magazzino
e ordini
Spedizioni
Conto
Stampante
Software
di cassa
Cassa
Stampante
Software
vendite online
Tablet
Gestionale
Magazzino
Gestionale
vendite online
WLAN ospiti
Server
Software
WLAN

Cloud

Mail WEB Internet

Fornitore

In linea

Portali

Valutazione del negozio

Fornitori di beni

Fornitori di servizi

Fornitori IT

Fornitore servizi di pagamento

Cassa malattia

Banca

WLAN ospiti

Server

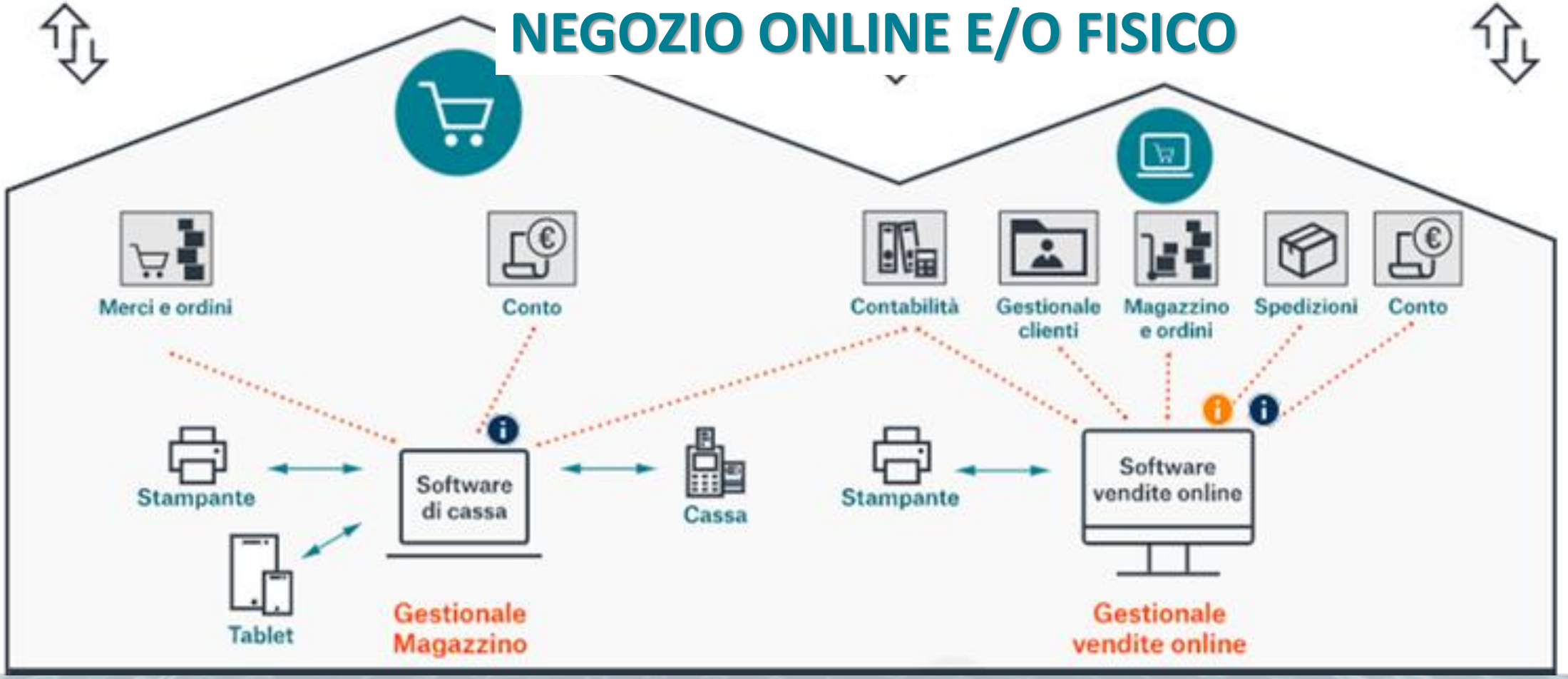
Software

Dati clienti

WLAN


Cloud
Mail
WEB
Internet
Fornitore
In linea
Portali
Valutazione del negozio
Fornitori di beni
Fornitori di servizi
Fornitori IT
Fornitore servizi di pagamento
Cassa malattia
Banca
Merci e ordini
Conto
Contabilità
Gestionale clienti
Magazzino e ordini
Spedizioni
Conto
Stampante
Software di cassa
Cassa
Stampante
Software vendite online
Tablet
Gestionale
Gestionale vendite online
WLAN ospiti
Server
Software
Dati clienti
WLAN

NEGOZIO ONLINE E/O FISICO



Scoperta dell'incidente

- Un cliente telefona: «Non riesco a fare acquisti nel negozio online»
- Chiede «Quando sarà di nuovo disponibile lo shop online?»
- Sul sito appare il messaggio "La pagina è momentaneamente non disponibile"

Conseguenze immediate

- Il titolare verifica: il sito web è effettivamente non raggiungibile
- L’attività di vendita del negozio online è bloccata
- Il titolare sospetta che possa trattarsi un attacco informatico

Azioni immediate

- Il titolare contatta il provider di servizi IT a cui è affidata la gestione “tecnica” del negozio online (servizi di web hosting)
- Il provider conferma: «Il negozio è offline già da 10 ore»
- Il provider comunica al titolare: «Ci vogliono almeno 24 ore prima di ripristinare il servizio»

Responsabile e sue motivazioni

- L’attacco è stato perpetrato da un concorrente con l’intenzione di avvantaggiarsene
- Per eseguire l’attacco il concorrente assume dei criminali informatici
- Nel darkweb vengono offerti numerosi “servizi” di questo tipo
- L’attacco perpetrato, che ha messo fuori uso il negozio online del titolare, è un cosiddetto attacco DdoS

Tipologia di attacco

- Il DdoS-Distributed Denial of Service è un metodo di attacco molto usato dai criminali informatici
- L'attacco DdoS consiste nel sovraccaricare un server saturandone le risorse
- La saturazione causa il malfunzionamento o il "collasso" del sito

Impatto

- Perdita di profitto dovuta all'interruzione dell'attività
- Perdita momentanea di clienti che effettuano gli acquisti su siti concorrenti
- Perdita permanente di clienti che passano al principale concorrente

ARTIGIANO – EDILE – CARPENTIERE - FALEGNAME

Scoperta dell'incidente

- Un dipendente si accorge che il computer non funziona, il sistema IT non si avvia
- Messaggio sullo schermo del PC: «Dati crittografati»
- Richiesta di riscatto online

Conseguenze immediate

- Bloccate le comunicazioni e-mail
- Impossibile accedere ai dati di clienti e dipendenti
- Impossibile accedere al gestionale
- Il software CAD e le macchine CNC sono bloccate

Azioni immediate

- I dipendenti informano il titolare
- Chiamano il provider IT
- Si tenta senza successo di ripristinare i dati dai backup

Responsabile e sue motivazioni

- Hacker ha crittografato i dati mediante un malware
- Richiesta di riscatto per decriptare i dati

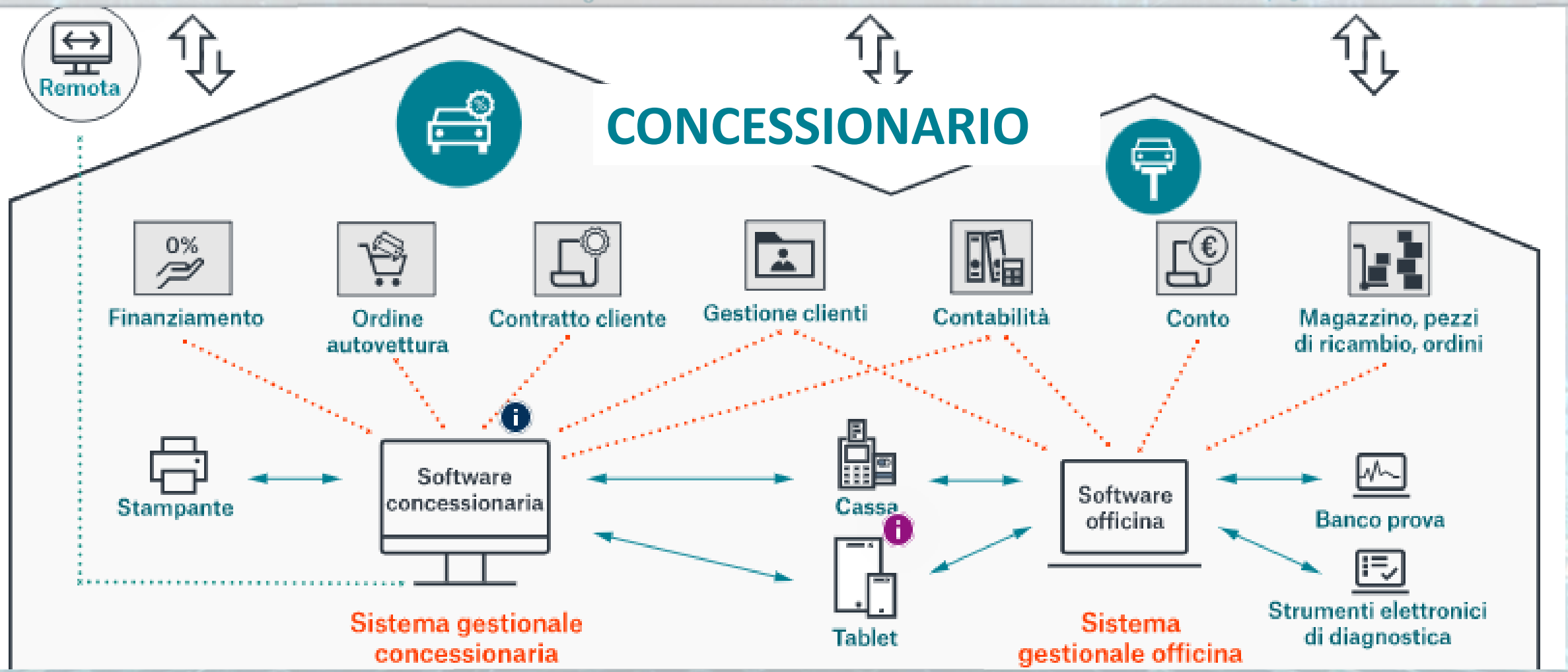
Tipologia di attacco

- Gli attacchi ransomware sfruttano due vulnerabilità principali: l'errore umano (dipendenti poco accorti) e la scarsa sicurezza dei sistemi
- Gli attacchi ransomware sono gli attacchi più comuni a livello mondiale
- L'ultima frontiera è il doppio ricatto: chiedere un riscatto per decriptare i dati e poi chiederne un altro per non pubblicare i dati rubati

Impatto

- Elevato stress per il titolare e i dipendenti
- Operatività compromessa / fatturazione di nuovo possibile solo dopo 4 settimane e conseguente perdita di profitto
- Costi da sostenere: eventuale riscatto, ripristino di dati e sistemi
- Spese: pagamento di eventuali sanzioni e adempimento degli obblighi previsti dal GDPR (es. obbligo di comunicazione)
- Danno di immagine e perdita dei clienti


STUDIO LEGALE
Remote
Scambio dati
Controllo
fatturazione eletronica
Conto
Stampante
Software studio legale
Tablet
Fax
Gestionale studio legale


Remota
CONCESSIONARIO
0%
Finanziamento
Ordine autovettura
Contratto cliente
Gestione clienti
Contabilità
Conto
Magazzino, pezzi di ricambio, ordini
Stampante
Software concessionaria
Cassa
Tablet
Software officina
Banco prova
Strumenti elettronici di diagnostica
Sistema gestionale concessionaria
Sistema gestionale officina

Scoperta dell'incidente

- Dipendente concessionario apre e-mail avente ad oggetto la presunta verniciatura di un veicolo
- Messaggio sul monitor: "Congelato"
- Sistema gestionale della concessionaria inutilizzabile
- Inutili i tentativi di riavviare i sistemi IT

Conseguenze immediate

- Impossibile accedere a sistema di posta, scadenzario, dati dei clienti e dati contabili
- Inutilizzabile anche il gestionale lato officina
- Impossibile accedere alle informazioni su magazzino e ordini

Azioni immediate

- Il titolare viene informato
- Tutti i PC vengono disconnessi dalla rete, in via precauzionale
- Il provider di servizi IT comprende immediatamente la gravità della situazione e chiede se sono disponibili backup (copie di sicurezza) recenti
- I backup erano memorizzati su supporti esterni; sono quindi intatti e risalgono a una settimana prima

Responsabile e sue motivazioni

- Un concorrente vuole danneggiare la concessionaria
- Per eseguire l’attacco il concorrente assume dei criminali informatici
- Nel darkweb vengono offerti numerosi “servizi” di questo tipo
- È stato inviato un virus che ha bloccato i sistemi e criptato i dati

Tipologia di attacco

- Gli attacchi ransomware sfruttano due vulnerabilità principali: l’errore umano (dipendenti poco accorti) e la scarsa sicurezza dei sistemi
- Vengono utilizzati indirizzi e-mail noti al destinatario (ad es. e-mail di partner commerciali)
- Il dipendente crede che l’e-mail sia sicura e apre l'allegato che contiene il virus
- L'attività viene bloccata anche per 10 giorni
- È possibile il ripristino di dati e sistemi grazie ai backup effettuati

Impatto

- Impossibile gestire lo scadenzario, coordinare o svolgere le attività
- Necessario pagare degli esperti di informatica forense per identificare la causa del danno e ripristinare i backup
- Necessario reinserire manualmente i dati dell'ultima settimana, in quanto non salvati sull'ultimo backup
- Perdita di profitto dovuta all'interruzione dell'attività
- Fatturazione è di nuovo possibile solo dopo 2 settimane: c'è quindi un problema di liquidità


Cloud
Mail
WEB
Internet
Fornitore
In linea
Portali
Valutazione del negozio
Fornitori di beni
Fornitori di servizi
Fornitori IT
Fornitore servizi di pagamento
Cassa malattia
Banca
HOTEL - RISTORANTE
Sistema chiavi elettroniche
Pulizie
Prenotazioni
Channel Manager
Revenue Manager
Contabilità
Lista Coronavirus
Prenotazioni
Stampante
Webcam
Software per hotel
Gestionale hotel
Tablet
Cassa
Orderman
Software ristorante
Gestionale ristorante
Distributori automatici
Ordine cucina
WLAN ospiti
Server
Software
WLAN

Scoperta dell'incidente

- Mentre cerca di fare check-in di un cliente, l'addetto della reception si accorge che il software non funziona più
- Messaggio sullo schermo del PC
- Dati crittografati
- Richiesta di riscatto online
- Il software dell'hotel non funziona più

Conseguenze immediate

- Impossibile effettuare check-in e check-out
- Chiavi elettroniche non funzionano
- Le prenotazioni non possono essere visualizzate
- Bloccate le comunicazioni e-mail
- L’hotel non è più operativo

Azioni immediate

- Il direttore dell'hotel viene informato
- Si tenta senza successo di ripristinare i dati mediante backup
- Viene chiamato il fornitore IT
- Viene informata la polizia

Responsabile e sue motivazioni

- Hacker crittografa i dati mediante un malware
- Richiesta di riscatto per decriptare i dati
- Gli hacker utilizzano ransomware sofisticati per questi attacchi
- Attacco spesso perpetrato contro PMI

Tipologia di attacco

- Gli attacchi ransomware sfruttano due vulnerabilità principali: l'errore umano (dipendenti poco accorti) e la scarsa sicurezza dei sistemi
- Gli attacchi ransomware sono gli attacchi più comuni a livello mondiale
- Profitto da richiesta di riscatto e da vendita di dati (ad esempio dati di carte di credito)

Impatto

- Elevato stress per personale dell’hotel e ospiti
- Operatività della struttura compromessa per più giorni
- Costi per pagamento riscatto e ripristino di dati e sistemi
- Sanzioni da pagare alla società emettitrice delle carte di credito
- Cancellazione di prenotazione per pubblicità negativa

GENERALE/BUSINESS	**1. Si sono verificate violazioni di sicurezza/incidenti informatici negli ultimi 3 anni che hanno determinato un impatto negativo?** **2. Fate attività di vendita attraverso E-Commerce?** **3. L'organizzazione seleziona i fornitori in base alle loro politiche di cyber security e di trattamento dei dati, e verifica periodicamente il mantenimento dei requisiti richiesti in ingresso?**
PROCESSO/ORGANIZZAZIONE	**4. Chi presidia la sicurezza informatica nell'organizzazione? Responsabile della Sicurezza Informatica, Responsabile IT, Responsabile delle operazioni, Responsabile sicurezza interna, Fornitore esterno (consulente), AD/proprietario, nessuno)** **5. Avete un responsabile della protezione dei dati (DPO)** **6. Formi il personale sui rischi cyber? Quale percentuale? Come... corsi, simulazioni, articoli, istruzioni scritte, ..., nulla)** **7. Fate fare ai vostri dipendenti smartworking? Utilizzate canali protetti con VPN?** **8. Avete fatto un piano di recovery in caso di attacco hacker? Coinvolgete i fornitori nei test di continuità operativa?**
DIGITALE/ INFORMATICA	**9. Utilizzate buone password? Quanto lunghe? Quanto spesso le cambiate? Quanto sono comuni a diversi tipologie di accessi?** **10. Fai un backup dei dati? Quanto frequentemente?** **11. Hai un provider IT esterno? Se si hai un contratto di manutenzione?** **12. Usi software esterno? Se si lo tieni sempre aggiornato?** **13. Utilizzate firewall per proteggere la rete?** **14. Quanto è digitale la vostra contabilità, la fatturazione e altre elaborazioni?**

riCONOSCI le vulnerabilità

Come e dove indicarle alle PMI

Attacco al database di un negozio online: rubati i dati dei clienti

Gli hacker decifrano la password del web server e rubano i dati dei clienti, a cui bisogna comunicare l'accaduto

- Sito italiano di e-commerce - Hacker, con un attacco cosiddetto "di forza bruta", entrano in possesso della password di accesso al web server rubano i dati delle carte di credito dei clienti
- Il fornitore IT spegne subito il sito web, controllano i dati del negozio presenti nel backup per verificare la presenza di eventuali malware e poi li ripristinano, rimuovono i file danneggiati e installano patch di sicurezza aggiornate per proteggere al meglio il sistema.
- Il negozio si ferma per 30 ore
- L'azienda informa in via precauzionale tutti i clienti, per controllare i singoli record di dati persi.

Ripartizione del danno (danno totale 12.950€)

- ❑ Ripristino negozio online **4.400€**
- ❑ Interruzione attività **1.250€**
- ❑ Indagine forense **1.300€**
- ❑ Comunicazione clienti **6.000€**

Costi coperti dalla compagnia di assicurazioni 12.950€

Criptati i dati di uno studio di otorinolaringoiatria

- Studio di otorinolaringoiatria ha registrato, nel proprio sistema informatico, 75.000 dati sui pazienti. Gli hacker attaccano il sistema con un Trojan e riescono a criptare parte dei dati che, nonostante l'utilizzo di due diversi sistemi di backup, i tecnici non riescono a ripristinare.
- Solo dopo un lungo lavoro i tecnici trovano un modo per ripristinare i dati dal backup, anche se solo parzialmente.
- La perdita di tutti i dati sarebbe costata tantissimo: la mancata presentazione dei dati di fatturazione avrebbe significato l'impossibilità di ricevere dal sistema sanitario pubblico i rimborsi per le prestazioni fornite, per un ammontare complessivo di € 75.000.
- Inoltre, se i dati fossero stati non solo criptati ma anche rubati, si sarebbero dovute mettere in atto procedure specifiche in materia di protezione dei dati.
- Il medico titolare dello studio non aveva l'assicurazione e, per sua stessa ammissione, l'incidente occorso è servito a fargli comprendere l'importanza di una adeguata copertura assicurativa. Della polizza ora sottoscritta apprezza in particolare il servizio di supporto che mette a disposizione esperti professionisti 24/7.

Ripartizione del danno (danno totale 12.000 €)

- ❑ Consulenza informatica e recupero dati — **12.000€**
- ❑ Potenziale perdita di guadagno — **75.000€**

Recupero dati: l'assicurazione assegna l'incarico a un tecnico specializzato e/o sostiene i costi corrispondenti, pari a € 12.000

Danno da perdita di profitto: se si fosse verificato, l'assicurazione lo avrebbe coperto per l'intero ammontare di € 75.000

Informativa ai pazienti: se necessaria in base al GDPR, l'assicurazione copre i costi.

Indagini forensi: l'assicurazione assegna l'incarico a un provider specializzato e/o sostiene i costi corrispondenti

Hacker ricattano un’autoconcessionaria

Ci sono voluti tre giorni per ritornare alla normale operatività.

- In azienda, 145 dipendenti su 185 dispongono di una postazione di lavoro con PC; lunedì mattina cercano di accendere i propri computer ma si accorgono subito di non poter accedere a molti file, tra cui quelli relativi alle riparazioni da eseguire sui veicoli, che vengono gestite attraverso il numero di telaio di ciascuna autovettura. I criminali hanno infettato i sistemi attraverso un malware inviato tramite e-mail e hanno così potuto criptare i dati aziendali.
- Il titolare non può far altro che verificare l’impossibilità di accedere ai dati, che fortunatamente sono stati “solo” criptati ma non sono andati persi, cosa che avrebbe comportato un danno incalcolabile per l'azienda.
- Gli hacker chiedono un riscatto di 150 Bitcoin, pari a circa 750.000 euro, ma l'azienda si rifiuta di pagare e ripristina i dati grazie ai backup, anche se il ripristino dei sistemi - e quindi la ripresa della normale operatività - richiede tre giorni.

Ripartizione del danno (danno totale 100,000€)

❑ Recupero dati	**12.000€**
❑ Interruzione dell’attività	**80.000€**
❑ Indagini forensi	**8.000€**

Costi coperti dalla compagnia di assicurazioni 100.000€

Cosa ne pensate: quanto è buona la vostra sicurezza informatica?

Qual è la probabilità che la vostra azienda possa essere colpita da un attacco informatico?

Utilizzate il vostro server o il cloud?

Utilizzate lo smartworking?

Quale software di settore utilizzate?

Avete un fornitore di servizi IT esterno? Se si avete un contratto di manutenzione?

Qual è la percentuale di clienti acquisiti per via digitale?

Quanto vi affidate all'IT per l'elaborazione degli ordini?

Quanto è digitale la vostra contabilità, la fatturazione e altre elaborazioni?

Formazione del personale sulle minacce alla sicurezza

Backup dei dati rilevanti dal punto di vista operativo

Industry average of all surveys: 33%

ndustry average of all surveys: 54%

Attenzione! Quando si utilizza il cloud, è necessario prestare particolare attenzione alla sua protezione con l'autenticazione a più fattori.

Il lavoro fuori dall'ufficio deve tenere lontani i potenziali "aggressori" attraverso un accesso al server ben protetto e garantire standard minimi in termini di sicurezza quando si utilizzano dispositivi finali privati per il lavoro d'ufficio.

l software di settore è di solito il perno digitale. Se questo viene criptato, ad esempio da un malware, di solito si verifica un'interruzione (almeno parziale) delle operazioni.

Descrizione

Il termine “malware” (= malicious software) indica tutti quei programmi che si diffondono tramite Internet ed espongono un computer a rischi sia in fatto di privacy che di funzionamento del sistema operativo. Malware è quindi un termine generico che comprende, tra l’altro, virus, trojan, worm, spyware, adware, rogueware.

Conseguenze

I malware sono in grado di corrompere i sistemi, danneggiare le reti, mettere a rischio le informazioni, eliminare o modificare dati e applicazioni, crittografare i database ecc.

Contromisure

Scansione dei sistemi con programmi anti-malware e antivirus

CAPIRE COME E DOVE INSERIRLO

Descrizione

Per “**software obsoleto**” si intende un software non aggiornato, cioè una versione più vecchia rispetto all’ultima release oppure l’ultima versione disponibile su cui però non siano state installate le ultime patch rilasciate dal produttore. Un software obsoleto presenta lacune e vulnerabilità soprattutto per quanto riguarda la sicurezza.

Conseguenze

L’utilizzo di software obsoleto permette agli hacker di accedere ai sistemi sfruttando le lacune degli stessi e di portare a termine attacchi informatici di vario tipo.

Contromisure

Aggiornamento regolare e tempestivo del software (sistemi operativi e applicativi) installando le patch di sicurezza.

CAPIRE COME E DOVE INSERIRLO

Descrizione

Il **ransomware** è un malware (cfr.) che può colpire i sistemi IT in maniera accidentale o intenzionale (attacco perpetrato da un criminale informatico). Il ransomware è in grado di criptare i file presenti sul computer della vittima, bloccandoli e richiedendo un riscatto per decriptarli.

Conseguenze

Esfiltrazione e manipolazione dei dati, blocco tramite crittografia, o eliminazione, di sistemi, applicazioni, informazioni.

Contromisure

Backup dei dati, protezione dei sistemi con programmi anti-malware e antivirus, maggiore consapevolezza degli utenti dei sistemi.

CAPIRE COME E DOVE INSERIRLO

Descrizione	Conseguenze	Contromisure
Furto di un dispositivo mobile per impossessarsi di hardware, software o dati sensibili del possessore.	Violazione delle responsabilità previste dal GDPR, pagamento di riscatto per evitare divulgazione dei dati, sostituzione dei dispositivi rubati, interruzione di attività.	Utilizzo di password e sistemi di crittografia, protezione fisica dei dispositivi mediante cavi e lucchetti di sicurezza, disattivazione delle porte USB, archiviazione dei dati su server centrale.

CAPIRE COME E DOVE INSERIRLO

Descrizione

Le e-mail di **phishing** e i siti web contraffatti sono entrambi strumenti che ingannano la vittima allo scopo di prendere controllo del suo computer e carpirne dati di accesso, eseguire malware o scaricare codice dannoso.

Conseguenze

Grazie a strumenti di ingegneria sociale incorporati, spionaggio, furto di identità, accesso ai dati delle carte di credito, accesso a dati di login (username, password) che permettono di entrare in una rete, ecc.

Contromisure

Aumentare la consapevolezza dei rischi connessi alla sicurezza informatica mediante formazione ed esercitazioni con simulazioni specifiche.

CAPIRE COME E DOVE INSERIRLO