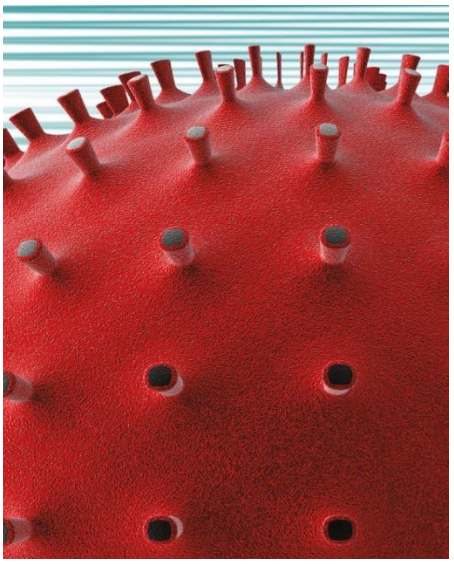
Zurich Commercial Insurance
Risk Insights

La dimensione Cyber del Coronavirus

Marzo 2020



Osservazioni

Nel corso delle ultime settimane, le aziende di tutto il mondo sono state colpite da un drastico aumento del numero di incidenti informatici.

Questa tendenza è stata recentemente confermata dall'emergere di attacchi legati al virus Covid-19. Secondo il CYE, una società specializzata nei servizi di sicurezza informatica e un partner di ZURICH, la situazione attuale è diventata, dall'inizio di febbraio, una nuova opportunità per gli hacker di approfittare dell'instabilità creata da questa pandemia globale. In effetti, il CYE osserva che il numero di casi si è moltiplicato per 5, una tendenza particolarmente marcata in Europa.

Sfruttando la preoccupazione generale, nonché il marcato cambiamento nel modo di lavorare e nell'organizzazione in relazione a questi eventi, la probabilità di aprire documenti "pericolosi" o l'uso di reti Internet non sicure per accedere ai dati sensibili fuori dall'ufficio continuano ad aumentare tra i dipendenti. I periodi di quarantena stanno diventando più frequenti, più lunghi e più diffusi, molti dipendenti sono autorizzati o addirittura costretti a lavorare in remoto. Questa nuova organizzazione richiede alle aziende di mantenere i controlli necessari a tutti i livelli dell'organizzazione aziendale.

Il "phishing" e altre campagne di "ransomware" hanno registrato un forte incremento nelle ultime settimane. Gli utenti cliccano su allegati o link dannosi inerenti il tema del Coronavirus.

Un recente attacco è arrivato sottoforma di messaggio proveniente dall' Organizzazione Mondiale della Sanità (OMS): un presunto impiegato dell''OMS ha richiesto informazioni di carattere personale e sensibili, tramite un allegato "infetto" che gli ha permesso di sottrarre informazioni di carattere personale.

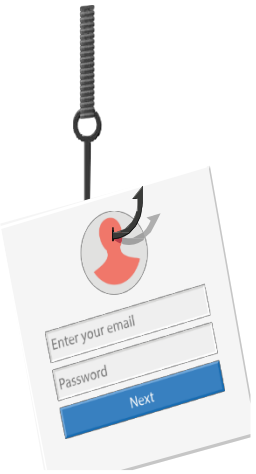


Figura 1: screenshot di una mail "infetta" che si presume provenga dall' OMS
- fonte: Proofpointinc

[1] https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/amp/

Esplosione dei rischi Cyber

Il lavoro a distanza e decentralizzato aumenta il rischio di rendere i dipendenti bersaglio di attacchi come quelli elencati di seguito:

Phishing / Spear phishing: Posta o altre comunicazioni elettroniche contenenti informazioni specifiche sul destinatario alfine di indurre il destinatario a cliccare su un link, aprire un allegato o qualsiasi altra azione che possa portare a compromettere i sistemi informatici o i dati.

Business E-mail Compromise (BEC): Azioni via e-mail finalizzate all'effettuazione di bonifici bancari, in genere tramite la personificazione del CEO, del CFO o di qualsiasi altro dirigente della società.

Social Engineering: Manipolazione psicologica dei dipendenti, inducendoli a compiere operazioni insolite.

Tutti questi eventi possono portare ad un aumento del rischio di domande di riscatto (ransomware), a causa di infezioni del computer, del blocco delle reti aziendali interne ed esterne e di crittografia o distruzione dei dati.

Dobbiamo essere coscienti che certi Cyber attacchi possono restare inattivi nei sistemi per alcuni giorni, mesi o addirittura anni. Le azioni intraprese oggi possono avere un impatto sulla reputazione e sulla performance finanziaria dell'azienda di domani.
Fortunatamente, ci sono anche diversi modi in cui le aziende e i dipendenti possono adottare misure preventive per evitare questi rischi e mantenere un ambiente digitale sicuro e protetto.

Raccomandazioni per ridurre i rischi:

Le persone:

Collegamenti/allegati: Non aprire i link o gli allegati contenuti nelle e-mail da fonti inaffidabili. Se i dipendenti desiderano navigare su un sito web, si consiglia di digitare l'indirizzo del sito direttamente nel browser. Un URL sicuro dovrebbe iniziare con il codice "https" invece di "http", ma questo non è sufficiente: è inoltre necessario che l'URL venga attentamente controllato prima di essere inserito nel motore di ricerca per assicurarsi che conduca al sito ufficiale dell'azienda/istituzione desiderata. In caso di dubbio, utilizzare un sito di verifica dell'URL, come **isitphishing.org.**

Informazioni: Non rispondere o dare informazioni su un conto o informazioni bancarie a una fonte sconosciuta. Le istituzioni affidabili, come i fornitori o i venditori, devono già disporre di queste informazioni. Non inviare mai informazioni di identificazione e/o password via e-mail a persone sconosciute o aprire documenti presenti nelle e-mail indesiderate.

Segnalare tutte le attività sospette: Tutte le e-mail sospette devono essere segnalate al team Cyber aziendale o al dipartimento equivalente.

Informare il team di supporto: Tutti i dipendenti devono contattare il servizio assistenza locale (help desk) se aprono un documento o un collegamento che potrebbe infettare il computer con malware.

Le aziende:

Formazione di sensibilizzazione dei dipendenti/utenti: Prima di autorizzare le connessioni remote alla rete aziendale, i dipendenti devono seguire una formazione adeguata inerente le campagne di phishing e sulle procedure di sicurezza. Devono inoltre conoscere tutti i processi e le procedure necessarie per segnalare un problema di sicurezza in caso di sospetto o identificazione di un attacco.

Connessioni sicure: Utilizzare unicamente una connessione remota sicura per accedere alle reti aziendali. Preferibilmente attraverso una rete privata virtuale (VPN) o qualsiasi altro meccanismo di connessione criptata.

Authentification Multifactorielle (AMF): Le connessioni VPN devono essere configurate con l'autenticazione a più fattori, che rappresenta un ulteriore livello di sicurezza per garantire che solo il personale autorizzato abbia accesso alla rete aziendale.

Gestione apparecchi portatili: I computer portatili (laptop), i tablet e gli smartphone dei dipendenti devono essere dotati di una soluzione di gestione dei dispositivi mobili. La soluzione deve applicare adeguati controlli di sicurezza e creare un ambiente virtuale criptato all'interno del dispositivo per memorizzare ed elaborare le informazioni aziendali.

Perimetro di protezione Internet:

I reparti IT devono assicurarsi che i firewall siano correttamente configurati e monitorare la registrazione del firewall per identificare i tentativi di connessione o gli esiti positivi di connessione da indirizzi IP (Internet Protocol) non autorizzati o sospetti.

Sicurezza e conformità Cloud:

Le aziende che utilizzano i servizi Cloud devono assicurarsi che le configurazioni di sicurezza siano adeguatamente rafforzate e monitorate per prevenire la deriva delle configurazioni o la manipolazione non autorizzata.

Rafforzamento dei controlli/vigilanza:

Se esistono aree geografiche o paesi in cui i dipendenti non hanno motivo di connettersi in remoto alla rete aziendale, il servizio informatico IT deve vietare in modo proattivo qualsiasi intervallo di indirizzi IP in tali aree geografiche, impedendo la connessione alle reti aziendali.

Ultime riflessioni e considerazioni

Concentrarsi su ciò che si può vedere è sempre stato parte della natura umana.
Il Coronavirus ci ricorda che l'invisibile e l'intoccabile a volte può essere molto più distruttivo dei rischi più tangibili che vediamo o di cui leggiamo quotidianamente (ad esempio, incendi, furti o incidenti stradali). I rischi informatici (Cyber), come il COVID-19, fanno parte della categoria dei rischi non tangibili. Negli ultimi anni abbiamo assistito a molti eventi segnati da virus digitali che hanno infettato una macchina dopo l'altra, creando una vera e propria pandemia in poco tempo.
L'incidente "NotPetya" del 2017 rappresenta la più grande pandemia mai verificatasi fino ad oggi, che ha colpito migliaia di aziende in tutto il mondo, con una perdita economica di quasi 10 miliardi di dollari. Ancora oggi l'igiene è fondamentale per evitare l'infezione. I sistemi a toppa (patch) e il lavaggio delle mani hanno la medesima importanza. Le sabbiere (Sandbox) e le quarantene hanno delle somiglianze sorprendenti quando si tratta di gestire il potenziale contagio.

In materia di cibernetica, il *National Institute of* Standards and Technology (NIST) fornisce un quadro alle aziende per sviluppare la loro capacità di identificare il rischio informatico, proteggere, rilevare, rispondere e recuperare da un attacco informatico. Queste capacità includono la tecnologia senza essere limitate a questa dimensione. Come già detto, la consapevolezza e le procedure messe in atto sono al centro della protezione. Un rilevamento affidabile e rapido, seguito da una risposta e da un recupero adeguati è fondamentale. La situazione attuale del COVID-19 ci offre anche le seguenti prospettive: Come gestire improvvisi aumenti della domanda di protezione? I disinfettanti per le mani e maschere sono diventati merce rara e il sistema sanitario è a malapena in grado di gestire il crescente numero di pazienti nelle unità di terapia intensiva.

Per cui, dobbiamo chiederci come questo si possa tradurre per la prossima pandemia cyber: possiamo dipendere dalla nostra protezione informatica e dalle nostre capacità di risposta? Possiamo contare su fornitori di servizi esterni in caso di una pandemia cyber - sapendo che offrono i loro servizi a diversi clienti e dovranno quindi fare una selezione e dare delle priorità a causa delle loro scarse risorse?

La nostra Cyber sicurezza interna e le nostre capacità di risposta alle emergenze sono sufficienti?

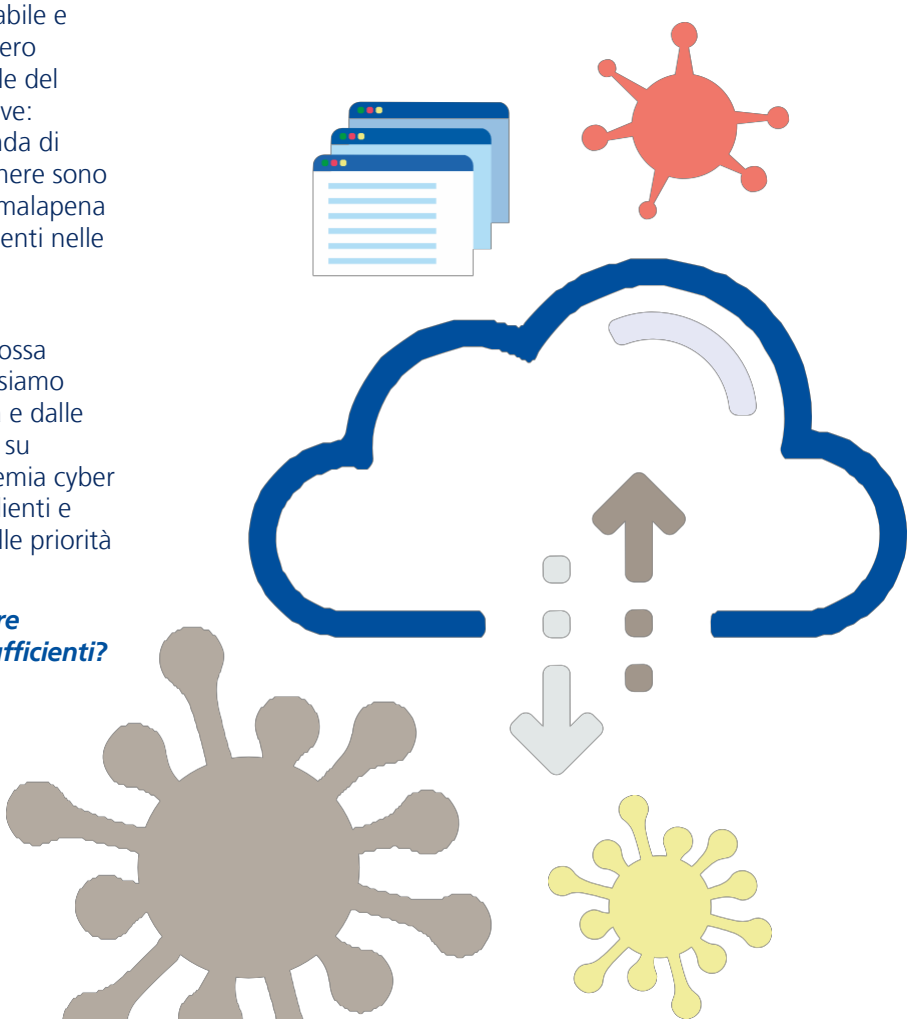
Il COVID-19 ci ha mostrato la complessità delle catene di approvvigionamento e la nostra dipendenza da beni intermedi importati da altri paesi e continenti. Oggi, questo non è più unicamente vero per i fornitori fisici, ma anche per tutti i fornitori informatici, d'archiviazione dati e piattaforme su cui le applicazioni possono operare.

Nel corso degli ultimi decenni, una delle principali tendenze nel settore manifatturiero è stata la delocalizzazione e in seguito dall'esternalizzazione dei servizi (outsourcing).

Nel campo della tecnologia informatica, il caso è lo stesso. Oggi il passaggio ai servizi cloud è il passo successivo e molte aziende stanno migrando le loro infrastrutture informatiche verso le piattaforme cloud dei principali fornitori (provider).

L'opportunità tecnica di lavorare in modo più redditizio (in termini di utilizzo o di costi) attraverso i servizi cloud ci aiuta a rispondere e a riprenderci da una vera pandemia, creando anche la prossima vulnerabilità invisibile e intangibile.

Mentre siamo ancora alla ricerca di un "interruttore" *(killswitch)* per COVID-19, possiamo già analizzare ciò che questo virus ci mostra sulla nostra resistenza digitale e sulla sicurezza informatica, nonché le aree di miglioramento in preparazione al prossimo virus cyber epidemico.



173006686 (03/20) TCL

ZURICH®