Dieci errori sulla sicurezza informatica che possono costare molto cari.

La criminalità informatica è diventata un tema talmente presente nella vita di tutti i giorni che noi ormai non facciamo più caso ai numerosi annunci sugli attacchi ransomware, alla violazione della privacy e ad altre truffe. Ma questo è un grave errore. La criminalità informatica è diventata un business lucrativo che genera miliardi di introiti. Poiché siamo un po' tutti coinvolti, è importante valutare il rischio in modo adeguato. Gli errori potrebbero costarci molto cari.

Errore numero 1_
Il ransomware è un attacco a 360 gradi – se lo superiamo, allora siamo al riparo.
Il ransomware è nella stragrande maggioranza dei casi solo il punto in cui gli aggressori fanno notare alla vittima che loro sono presenti in loco e quello che hanno fatto. Gli aggressori erano probabilmente presenti in rete già da giorni, se non da settimane, prima di procedere all'attivazione del ransomware. In tutto quel tempo hanno esplorato la rete, disattivato o cancellato i backup, trovato computer con informazioni o applicazioni importanti, rimosso informazioni e installato payload o backdoors supplementari. Il fatto che le vittime rimangano in rete, permette agli aggressori di sferrare un secondo attacco – in qualsiasi momento.

Errore numero 2_
Il pagamento di un riscatto ripristinerà i nostri dati.
Il pagamento del riscatto non è una soluzione per rimettersi in piedi – anche se sembra essere l'opzione più semplice. Secondo il rilevamento „State of Ransomware" del 2021, le aziende che hanno pagato il riscatto hanno potuto recuperare solo circa il 65 percento dei loro dati. Solo l'otto percento ha avuto indietro tutti i propri dati, e il 29 percento ha potuto ripristinare meno della metà di questi. Inoltre il ripristino dei dati è solo una parte del processo di recupero – nella maggior parte dei casi il ransomware blocca completamente il computer, ragion per cui il software e i sistemi devono essere reinstallati da zero, prima che i dati possano venire ripristinati. I costi da sostenere per tale ripristino sono in media dieci volte maggiori di quelli della richiesta di riscatto.

Errore numero 3_
Abbiamo un firewall. Perciò il nostro IT è ben al sicuro contro ogni attacco.
È compito specifico del firewall, verificare e filtrare di continuo il traffico di dati tra le reti interne ed esterne. Questo deve al contempo mettere in stato di allarme il personale IT chiave dell'azienda o il fornitore di servizi IT esterno in caso di malfunzionamenti o attacchi informatici. Tuttavia un firewall da se non basta a rendere sicura la vostra organizzazione in modo efficace. Ad esempio i dati che gli utenti caricano sul computer tramite la chiavetta USB non vengono rilevati dal firewall. Questi sono quindi una potenziale via d'accesso per software che danneggiano l'intero sistema. Il firewall è anche non in grado di impedire una gestione scorretta dei dati login (ad esempio in caso di un attacco phishing).

Errore numero 4_
La sicurezza è compito del reparto IT.
Fin troppo spesso il tema riguardante la sicurezza viene delegato ai responsabili del settore IT. Oppure l'azienda confida nel fatto che il partner IT svolga il proprio lavoro correttamente – senza giungere a regolare chiaramente gli specifici ambiti di responsabilità. Non è un caso raro che si verifichino importanti attacchi alle interfacce perché queste non sono state ben definite oppure ci sono stati dei fraintendimenti. In caso di attacco informatico, ne risponde direttamente l'azienda. Il consiglio di amministrazione ed eventualmente anche la direzione potrebbero essere accusati di aver adottato insufficienti misure di protezione in caso di danni causati da un attacco informatico. Tale accusa non può venire estesa ai responsabili del settore IT, né ovviamente a personale esterno. La sicurezza del settore IT dovrebbe perciò essere considerata dalla direzione come un tema strategico di grandissi ma importanza.

Errore numero 5_
Non affido la sicurezza ad altri. Questo tema è troppo importante per me.
In modo specifico per le PMI non è possibile tenersi di continuo aggiornati su tutte le novità sulla

sicurezza informatica. Quindi non si possono adottare i provvedimenti immediatamente necessari a causa della presenza di una nuova tipologia di minacce. Inoltre ci sono solo poche PMI in grado di monitorare la propria infrastruttura IT e di reagire prontamente in caso di contrattempi con il loro sistema di protezione. Persino anche quando l'azienda dispone di un suo team IT, merita collaborare con un partner esterno che si occupa di sicurezza IT – così il proprio reparto IT si può concentrare su progetti IT di una certa rilevanza dal punto di vista commerciale.

Errore numero 6_
Non siamo interessanti per gli hacker e non abbiamo segreti.
Molte vittime di attacchi informatici si ritengono irrilevanti, troppo poco interessanti o poco lucrativi per essere minacciati. Ma i criminali non se ne preoccupano. Ogni persona o piccola impresa con una presenza digitale e utilizzo di computer è una potenziale vittima. La maggior parte degli attacchi sferrati dagli hacker non sono spettacolari, ma vengono effettuati da opportunisti alla ricerca di possibili vittime. Il loro target preferito sono aziende con sistemi di sicurezza non aggiornati o configurazioni errate. Chi ritiene di essere un bersaglio insignificante, dovrebbe già ora perlustrare a fondo la sua rete in cerca di attività sospette.

Errore numero 7_
Abbiamo un piano di emergenza.
Avere un piano di emergenza è di fatto molto importante. Con ciò viene garantito che voi o il vostro IT in caso di un attacco informatico possiate adottare misure di sicurezza adeguate e reagire prontamente. Questo piano può contenere istruzioni su come potere separare velocemente un server dalla rete, qualora doveste essere vittima di un attacco. Nel caso di un attacco informatico, reagire rapidamente è uno dei più importanti fattori per ridurre al minimo i danni che ne conseguono. Ciononostante, un piano di emergenza non basta a garantire una vera e propria protezione. È piuttosto una salvaguardia per evitare danni maggiori. La protezione deve essere proattiva. Un piano di emergenza è sempre reattivo.

Errore numero 8_
Abbiamo un'assicurazione.
Un'assicurazione non basta purtroppo a proteggervi. Tra l'altro paga di regola al massimo il danno monetario. Le misure proattive di Cyber Security sono come i freni in un veicolo. Nessuno rinuncia ai freni solo perché il veicolo è assicurato.

Errore numero 9_
I nostri dipendenti vengono continuamente aggiornati sulla materia, e questo basta.
I nostri dipendenti vengono continuamente aggiornati sulla materia, e questo basta. Secondo lo studio „State of Ransomware 2021" il 22 percento delle aziende ritiene di potere essere vittima di un ransomware nei prossimi dodici mesi. Tecniche di social engineering come le e-mail phishing sono sempre più difficili da riconoscere. I messaggi sono spesso scritti in modo così specifico, convincente e accurato, che per i dipendenti è quasi impossibile riconoscere la loro vera natura. Ovviamente molti attacchi possono essere respinti grazie a regolari campagne di aggiornamento rivolte ai dipendenti. Ciononostante, tale aggiornamento dovrebbe essere parte integrante di una vasta strategia di sicurezza informatica.

Errore numero 10_
Ogni dipendente risponde di persona.
Per le aziende sono i dipendenti che rispondono in prima persona della gestione sicura delle e-mails e Internet. In effetti sta all'azienda sensibilizzare i propri dipendenti sulla tematica dei rischi legati alla sicurezza informatica, proprio come indossare le scarpe antinfortunistiche o il casco in cantiere. È dovere del dipendente utilizzare in modo appropriato e in qualsiasi momento i tools che gli vengono forniti.

Sicurezza informatica di UMB

Grazie a servizi di sicurezza informatica modulari, UMB crea protezione permanente in un mondo sempre più complesso e digitale. Solo interventi organizzativi e tecnici equilibrati possono proteggere la vostra azienda in modo olistico ed efficace. Per questo devono essere introdotte dimensioni di sicurezza nuove a completamento della prevenzione classica (protezione della rete e del perimetro). Questo vuol dire da una parte avere la capacità di rilevare per tempo la presenza di un aggressore. Dall'altra devono essere avviate rapidamente le contromisure adeguate.

IBM Platinum Business Partner

Sembra eccitante? Contattateci!

Siamo felici di rispondere alle sue domande sulla sicurezza informatica e altro.

Contatta
Markus Kaegi, Senior Security Consultant
markus.kaegi@umb.ch, +41 44 805 14 47, www.umb.ch