WEBINAR CYBERSECURITY

SPECIALTY PER GOMMA

FOCUS SILICONE

L'INDUSTRIA DELLA GOMMA

MENSILE DEGLI ELASTOMERI E DEGLI ALTRI POLIMERI RESILIENTI • *Maggio 2021*

688

Come proteggersi dal rischio cyber

Biesse Broker è un broker assicurativo specializzato in rischi industriali che collabora con circa 20 compagnie assicurative, italiane e internazionali. Da qualche anno sta approfondendo le tematiche sui rischi cyber. Maurizio e Massimo Modina ci introducono all'argomento

La tecnologia e la digitalizzazione avanzano e offrono grandissime opportunità di business alle imprese, ma le espongono anche a una maggiore possibilità di subire attacchi informatici. E se questi attacchi, fino a poco tempo fa, impattavano prevalentemente sulla parte amministrativa delle aziende, oggi più che mai possono invece pesare sull'intero processo produttivo, a causa dell'interconnessione tra sistemi IT e OT.
Si parla ormai da anni di questo tipo di vulnerabilità. Allianz, che ogni anno produce un report sui rischi maggiormente percepiti dalle imprese, nel 2020 lo collocava al primo posto tra quelli più temuti a livello globale. Nel rapporto 2021 è indicato anche tra i primi rischi percepiti dalle aziende italiane. Il 2020 è stato anche un anno che ha fatto registrare un forte incremento degli attacchi informatici, circa il 246% in più rispetto al 2019 in Italia.

LO SMART WORKING E UN MERCATO AGLI INIZI

Questo fenomeno è dovuto anche al fatto che le aziende hanno dovuto affrontare l'emergenza sanitaria incentivando lo smart working, o lavoro da casa. Ma non tutte erano pronte.
Ciononostante, circa il 73% delle imprese italiane ignora le polizze cyber o, comunque, non ne ha adottata una. Ciò accade perché, perlomeno in Italia, il mercato assicurativo, per quanto riguarda questo problema, è ancora giovane. I grandi gruppi hanno messo a disposizione solo da qualche anno polizze per i loro clienti che contemplano anche questo aspetto, al contrario di compagnie che invece sono specializzate su queste tipologie di rischi e che hanno sviluppato non soltanto prodotti specifici, ma anche e soprattutto l'esperienza nella gestione dei sinistri cyber, sempre caratterizzati da un elevato grado di complessità.
Inoltre moltissime aziende ancora oggi sottovalutano la possibilità di essere colpiti da un attacco informatico.

DA CYBER RISK A CYBER SECURE

Quello che possiamo fare oggi è aiutare le imprese a passare da una condizione di "cyber risk" a una di "cyber secure", in particolare avvalendoci della nostra esperienza e conoscenza del mercato per cercare una copertura assicurativa adatta e su misura per le necessità specifiche di una singola realtà. Per esempio, per tutelarla dalle principali spese a cui può andare incontro, come quelle di ripristino del sistema o per i danni da fermo di attività, ma anche per eventuali richieste di risarcimento che possono provenire dall'esterno, per esempio per la perdita dei dati e la violazione della privacy. Altri costi possono essere riguardare le spese legali, di notifica o necessarie per indagini forensi.
Ma soprattutto, una copertura cyber deve anche contemplare un'assistenza e mettere a disposizione un servizio di "incident response". In questo caso, società esperte di cybersecurity, collaborano insieme con l'azienda colpita e il suo reparto IT per eradicare gli eventuali malware, oltre a bonificare e verificare il sistema al fine di evitare un nuovo attacco.

SERVIZI PER LA PREVENZIONE

Altri servizi che offriamo, in collaborazione con partner, possono avere una funzione preventiva, per esempio attraverso test di vulnerabilità, per in-

dividuare eventuali criticità nell'infrastruttura, o per valutare, insieme con l'azienda, l'adozione di sistemi di monitoraggio attivi 24 ore su 24, i cosiddetti Security Operation Center. Oltre a ciò sono disponibili anche servizi per la prevenzione degli attacchi di phishing.

POLIZZA SU MISURA E ASSISTENZA

Interloquire con le aziende medie e piccole su questi temi è sempre complicato, per la percezione che spesso le aziende hanno di non essere interessanti per gli hacker. In realtà questa è una falsa sicurezza, perché ormai è dimostrato come gli attacchi non siano praticamente più mirati su specifiche realtà, ma siano lanciati su larga scala sul web con un concetto simile a quello della pesca a strascico, cioè orientato a catturare nella rete il maggior numero di malcapitati. In che modo allora avviene l'approccio con le imprese per illustrare loro il rischio cyber? Massimo Modina indica l'approccio utilizzato da Biesse Broker. «Noi cerchiamo di affrontare la gestione di questo rischio offrendo una risposta articolata», dice Modina. «Da un lato è importante un contratto assicurativo, perché assicura una sorta di seconda linea difensiva dietro a quella tecnologica. Per un buon contratto assicurativo sono importanti le garanzie, la personalizzazione in base alle specifiche esigenze dell'azienda e, naturalmente, il massimale di copertura. Altro elemento è poi quello delle attività di incident response, che servono soprattutto quando si subisce un attacco. È infatti fondamentale non farsi trovare impreparati, per intervenire in modo tempestivo dopo un attacco o un data breach».

I SERVIZI DI INCIDENT RESPONSE

Di fatto le società che forniscono servizi di incident response compresi nelle polizze assicurative sono esperte nell'individuare i tipi di malware. Giusto per avere un'idea, esistono oltre 34 diversi tipi di ransomware oggi in circolazione sulla rete ed è importante capire con che cosa si ha a che fare e quali sono i problemi connessi. «Il contratto assicurativo non basta», sottolinea Modina. «È importante anche capire il livello di esposizione al rischio. Al riguardo consigliamo i test di vulnerabilità. Ne esistono di diversi e si basano su scansioni effettuate con software specifici, che possono fornire informazioni interessanti, come per esempio individuare dati di proprietà dell'azienda finiti sul "dark web" o attività di download critiche. Le prime risultanze di queste indagini possono poi essere affinate con "penetration test" più approfonditi».

DAL PHISHING ALLA RILEVAZIONE DEGLI ATTACCHI

«Un altro aspetto a cui prestiamo molta attenzione», continua Massimo Modina, «è il rischio di phishing, uno dei problemi più seri con cui si può avere a che fare, che può comportare il furto di dati e anche, cosa interessante per le imprese del comparto gomma, il rischio che dalla posta elettronica e da password deboli il cyber criminale possa inserirsi nella rete aziendale e avere accesso a macchine di produzione, come le presse, per arrivare a bloccare la produzione. Esistono quindi simulazioni per il phishing, realizzate con i dipendenti delle aziende, per valutare l'entità di questo rischio».

Un terzo aspetto importante, sempre secondo Biesse Broker, «riguarda i sistemi di rilevazione degli attacchi informatici. Se si tratta di un ransomware il riconoscimento dell'offesa può essere anche immediato, ma in caso di furto di dati potrebbero servire anche settimane. La raccomandazione più importante, in definitiva, è di non sottovalutare questo rischio».

Un semplice test, che partendo da un indirizzo IP e da un nome di dominio di un sito può individuare eventuali porte aperte nel sistema informatico, è disponibile gratuitamente per i partecipanti al webinar. ◆