Hur mycket kostar intrånget? Ny tjänst från F-Secure ger svaret.

Nya Cyber Breach Impact Quantification beräknar skadan innan den inträffat, vilket ger beslutsfattare ett utmärkt underlag för att fatta rätt beslut om säkerhetsinsatser.

Helsingfors – 13 september, 2017: Hur mycket kostar ett intrång? Beroende på vart du riktat frågan, någonstans mellan 2 miljoner och 35 miljoner kronor* - ibland ännu högre. Den typen av uppskattningar kan vara användbara när det handlar om att skaffa sig en övergripande bild, eller att följa utvecklingen i ett historiskt perspektiv. Men när det gäller att förutse effekterna av ett intrång för en enskild organisation, eller ett specifikt företag, så är de helt meningslösa. För att hjälpa företag att förutse och bättre hantera sina risker lanserar F-Secure nu Cyber Breach Impact Quantification (CBIQ), en ny tjänst som uppskattar hur mycket ett intrång eller en säkerhetsincident skulle kosta.

De uppskattningar som F-Secures experter på riskhantering gjort visar att de flesta större organisationer är dåligt förberedda på att hantera ett intrång. Omkring hälften har ett krishanteringsteam som är redo för att hantera fysiska katastrofer, eller andra icke-planerade avbrott i affärsverksamheten – men bara 20 procent säger sig vara förberedda på en cyber-kris. 65 procent av företagen har aldrig kört någon form av övning i hur man hanterar ett intrång eller annan cyberincident.

Att sätta en prislapp på ett potentiellt intrång kan hjälpa företag och organisationer att ta tag i problemet och faktiskt bli mer förberedda och bättre på att hantera en incident.

”Företag tror att det är för komplicerat att beräkna kostnaden för cyberhot och -incidenter så de investerar miljoner i alla möjliga typer av säkerhetslösningar, bara för att kunna känna att de gjort allt de kan, säger **Marko Buuri**, riskhanteringskonsult på F-Secure. ”Men investeringarna kan göras på fel ställen, och när det verkligen sker ett intrång så står de helt handfallna. CBIQ tar bort mycket av osäkerheten – så att de vet vilken nivå de bör lägga sina investeringar på, samt var de bör göra dem.”

Att förutspå kostnaden för ett intrång innan det sker ger beslutfattarna en bild av *hur mycket* som verkligen står på spel, vilket ger dem ett mer fullständigt underlag så att de kan fatta mer välgrundade beslut. Det ger dem möjlighet att rikta insatserna dit de gör mest nytta och ger dem samtidigt något de kan använda för att rättfärdiga sina satsningar och dess kostnader för övriga delar av organisationen.

Expertkunskap + skräddarsytt simulatorverktyg = resultat som du kan lita på

När F-Secure utför en CBIQ-analys börjar säkerhetskonsulterna med en workshop och djupintervjuer med nyckelpersoner som kan ge en korrekt inblick i den aktuella organisationen och hur den är organiserad. De tar in alla olika typer av kostnader som är förenligt med ett intrång – IT-forensisk undersökning, återställning av system och tjänster, legala aspekter, kommunikationskostnader och, självklart, eventuella avbrott i affärskritisk verksamhet.

Konsulterna matar in all information i F-Secures skräddarsydda simulationsverktyg som beräknar möjliga utkomster och avgör median- och standardavvikelser i realtid. Verktyget är framtaget med mångårig erfarenhet av att undersöka intrång och att hjälpa företag med att återhämta sig när det inträffat. Det ger snabbt och kostnadseffektivt resultat och matar ut visuellt tydliga och lättförståeliga rapporter. CBIQ levererar en riskanalys som är baserad på hur företaget är uppbyggt, hur dess kostnadsstruktur ser ut och vilka förluster som kan väntas.

Enligt Marko Buuri skiljer sig CBIQ-metoden från det traditionella sättet att, exempelvis med Excel-ark av varierande komplexitet, redovisa risker i grovhuggna kategorier som hög, medium och låg.

”Där andra verktyg ger vaga resultat som är lätta att hitta invändningar mot så levererar vi tydliga siffror som bygger på transparent data från den egna organisationen. Varför ska man nöja sig med gissningar när det går att ta fram en riskanalys som faktiskt klarar av att stå emot en granskning?”

CBIQ är en del av F-Secures heltäckande tjänsteportfölj inom riskhantering. Bland tjänsterna finns exempelvis Incident Response Maturity Assesments, där företagets konsulter tar fram en helhetsbild av företagets säkerhetsarbete och gör en bedömning av mognadsgraden samt hur motståndskraftig organisationen är, samt olika tjänster för att ta fram nya processer, krishanteringsövningar, riskmodellering, workshop och utbildning.

**Rand Corp. uppskattar genomsnittskostnaden för ett dataintrång till 200 000 euro: https://www.rand.org/pubs/external_publications/EP66656.html. The Ponemon Institute sätter sin uppskattning till 3,6 miljoner dollar: https://www.ibm.com/security/data-breach/*

Läs mer:
F-Secure Risk and Security Management Advisory Services

Presskontakt
Adam Erlandsson
Cohn & Wolfe för F-Secure
+46 735 18 24 80
adam.erlandsson@cohnwolfe.com

Om F-Secure
Ingen kan cybersäkerhet som F-Secure. Under de senaste tre decennierna har F-Secure varit ledande inom innovation, samtidigt som man skyddar tiotusentals företag och miljoner människor. Företagets erfarenhet inom klientskydd och upptäckt och hantering av incidenter saknar motstycke och F-Secure skyddar företag och konsumenter från allt från avancerade cyberattacker och dataintrång till utspridda ransomware-infektioner. F-Secure erbjuder sofistikerad teknologi som kombinerar styrkan hos maskininlärning med den mänskliga expertis som finns i deras säkerhetslabb som uppmärksammats världen över i ett koncept de kallar Live Security. F-Secures säkerhetsexperter har deltagit i fler europeiska utredningar av cybersäkerhetsbrott än något annat företag och deras produkter säljs över hela världen av fler än 200 bredbandsleverantörer och mobiloperatörer samt tusentals återförsäljare.

Grundat 1988, F-Secure är listat på NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | facebook.com/f-secure