Den mänskliga sidan av cybersäkerhet

Föreställ dig det värsta som kan hända.

Hela ditt datacenter har stängts ner på grund av en sofistikerad utpressningsvirusattack. Försäljning, kundtjänst och ekonomi fungerar inte. Du är en senior IT-chef som ansvarar för att återställa systemen, men att hitta en lösning visar sig vara svårt.

Ditt team, som redan är hårt belastat, har arbetat veckor i sträck med mycket få raster eller ledig tid. Vissa teammedlemmar har ***arbetat så mycket som 36 timmar i sträck*** utan sömn. Du börjar bli orolig för att trötthet leder till dåligt beslutsfattande, något som i sin tur kan riskera själva återställningsinsatsen.

Du behöver desperat ytterligare resurser som omedelbart kan hoppa in och hjälpa till att lösa problemet, men var hittar du dem?

Det här scenariot kan låta som början på en roman men det är baserat på verkliga erfarenheter från Dells kunder. Det belyser ett betydande problem i dagens cybersäkerhetsmiljö: den mänskliga faktorn.

Nya data tyder på att branschen saknar nästan fem miljoner säkerhetsexperter. Resursbehoven känns som mest akuta under en incident, men lösningarna måste sätta in mycket tidigare.

Börja med att utveckla en strategi för rekrytering av nya talanger

Det första steget för att säkerställa att du har de resurser du behöver är att skapa en strategi för rekrytering av nya talanger:

Rekrytera på universitet och erbjud praktik

Genom att samarbeta med universitet och högskolor kan du hitta en stadig ström av unga talanger. Dessa personer kan utbildas till duktiga teammedlemmar över tid.

Löpande utbildning och utveckling

Tid och budget är under ständig press men cybersäkerhetsexperter måste hålla jämna steg med förändringar av både verktyg och hot.

Fokusera på att få medarbetarna att stanna kvar

Duktiga medarbetare efterfrågas alltid, särskilt om de har erfarenhet av att hantera en attack. Om du inte behåller dina topptalanger gör någon annan det.

Kanske inte ens ett starkt team klarar av att hantera all stress som en attack innebär. Då måste du planera framåt genom att identifiera ytterligare support innan det behövs:

Utvärdera resurser från tredje part

Konsult- och bemanningsföretag inom cybersäkerhet kan hjälpa ditt team både under pågående drift och när incidenter inträffar. Skapa relationer med dessa företag, även om du inte behöver dem nu, så att du har tillgång till dessa resurser när det behövs.

Dell erbjuder ett antal tjänster som kan förstärka befintliga team, inklusive virtuell CISO (vCISO), incidenthantering och cybersäkerhetsrådgivning.

Dra nytta av AI

Dra nytta av de nya AI-funktioner som byggs in i cybersäkerhetsverktyg som logganalys, avvikelsedetektering, prioritering av varningar på låg nivå eller specialiserad utbildning. På så sätt kan du klara resursbrist, hantera driftsbehov och frigöra teammedlemmar så att de kan fokusera på mer komplexa arbetsuppgifter.

Resursutmaningarna är som störst under en cyberattack

Som det första scenariot visade kan en större cyberattack lamslå ditt företag och paralysera viktiga system och verksamheter. Varje minut kostar företaget pengar och cybersäkerhetsteamet ställs inför en enorm press att åtgärda problemet.

Då är det viktigt att du ser till så att dina team är så uppdaterade som möjligt. Det har en direkt inverkan på incidenthanteringen och teamets stressnivå.

Tänk på att utbildningen måste sträcka sig bortom säkerhetsproffsen till alla medarbetare eftersom de är den första försvarslinjen.

Den här berättelsen understryker en viktig utmaning: cyberförsvararna är bara människor. De har gränser, och när dessa gränser överskrids kan även de mest professionella medarbetarna misslyckas. Mental trötthet, stress och utbrändhet är nu kritiska faktorer för cybersäkerheten.

Även om det kanske inte finns en enda lösning på denna utmaning kan följande strategier räcka långt:

Bygg upp ett starkt team och en strategi för att rekrytera nya talanger

Den mest grundläggande lösningen på det här problemet är att inte låta det bli en nödsituation – bygg upp ett starkt team med säkerhetsmarginaler på plats.

Planera för den mänskliga faktorn vid en attack

Incidenthanteringsplaner är avgörande och de MÅSTE innehålla planer för hantering av personal, schemaläggning och hantering av driftavbrott för anställda.

Utnyttja resurser från tredje part

Externa cybersäkerhetskonsulter kan hjälpa dig att förstärka ditt team. Med Dells incidenthanteringstjänster kan till exempel ett expertteam vara på plats inom några timmar – redo att bedöma, begränsa och påbörja åtgärder omedelbart. Vi har hjälpt många kunder att klara sig genom cyberattacker.

AI kan hjälpa men det är ingen universallösning

AI har stor potential att förbättra verktyg och program inom cybersäkerhet. AI kommer så småningom att kunna klara allt från prediktiv analys till att ta fram anpassade utbildningsprogram och till och med stoppa hot innan de hinner spridas.

Ännu viktigare är kanske att AI kan erbjuda försvararna ett stödsystem i realtid vid en incident. Maskininlärningsmodeller som tränats på data från tidigare attacker kan rekommendera åtgärder baserat på liknande händelser.

I takt med att bearbetning av naturligt språk blir en del av cybersäkerhetsverktyg kan analytiker interagera direkt med systemen, identifiera hot och driftsätta lösningar.

AI kan även följa beteendemönster och varna när en analytiker gör upprepade misstag – till exempel på grund av trötthet – och föreslå ett skiftbyte eller att någon annan tar över.

Cybersäkerhetsverktyg får snabbt mer avancerade AI-funktioner, men många av de mest kraftfulla möjligheterna håller fortfarande på att utvecklas. Tänk på att AI än så länge inte kan ersätta en erfaren expert, ***särskilt inte en person som har upplevt en attack tidigare***.

Tips för att utnyttja AI:

Lär dig hur verktygen kan hjälpa i ditt säkerhetsarbete

Gör en detaljerad analys av AI-verktyg och använd dem där de kan vara mest effektiva. Enkla sätt att potentiellt snabbt kunna dra nytta av AI kan vara avancerad hotdetektering, automatisering av upprepade uppgifter och AI inom identitetshantering.

> Den allra bästa metoden är att ha en partner som sköter incidenthantering, åtgärder och återställning.”
>
> ***Jason Rosselot***
> *VP, Cybersecurity and Business Unit Security Officer, Dell Technologies*

Planera för en framtid med AI

Ta reda på när nya funktioner blir tillgängliga, hur de gynnar ditt team och utveckla en plan för att implementera dem.

Använd AI i planeringen av arbetsstyrkan

I takt med att automatisering minskar mängden manuella uppgifter kan säkerhetsteamets sammansättning behöva utvecklas. Du kan behöva resurser på högre nivå för att analysera och agera på säkerhetsinformation, snarare än bara samla in den. Anpassa dina anställnings- och utvecklingsstrategier med det i åtanke.

AI kommer att spela en viktig roll i ditt cybersäkerhetsarbete, om den inte redan gör det. Men tänk på att AI inte kan ersätta en kunnig och erfaren expert. Målet bör vara att använda AI för att automatisera driften och göra personalresurserna mer effektiva. Det kan i slutändan förhindra attacker och minimera deras påverkan när de inträffar.

Förbättra cybersäkerhetsmognad ett steg i taget

Precis som allt inom cybersäkerhet är hantering av den mänskliga faktorn en resa och inte slutdestinationen. Små, stegvisa insatser gör skillnad och bygger upp framsteg med tiden. Det viktigaste att tänka på är att även de bästa tekniska lösningarna och säkerhetsverktygen bara är lika effektiva som människorna som hanterar dem.

DELL Technologies

Dell-produkter och -lösningar som kan hjälpa dig

Dells utvalda lösning	Beskrivning
Incidenthanteringstjänster	Ett team av branschcertifierade cybersäkerhetsexperter står redo för snabb insats vid en cyberattack. Vi samarbetar med dig för att eliminera hoten tills verksamheten är tillbaka till det normala.
Rådgivningstjänster för cybersäkerhet	Expertråd som kan hjälpa dig att hitta och åtgärda svaga punkter i din säkerhetsstrategi, skydda dina tillgångar och data och möjliggöra kontinuerlig vaksamhet och styrning.
vCISO	Chef för virtuell informationssäkerhet och cybersäkerhetsexpert som kan hjälpa till att identifiera och hantera risker samt vägleda strategiska beslut.
Managed Detection and Response	De minskar manuellt arbete och gör det dagliga säkerhetsarbetet smidigare genom att övervaka, upptäcka hot, utreda och snabbt reagera på slutpunkter, nätverk och i molnet. Kunder väljer den XDR-plattform de föredrar (Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR eller Microsoft Defender XDR) och får expertrådgivning, kvartalsrapporter och upp till 40 timmars årlig incidenthantering.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **dell.com/cybersecuritymonth**

DELL Technologies