De menselijke kant van cyberbeveiliging

Stelt u zich het ergste scenario voor.

Uw volledige datacenter is platgelegd door een geavanceerde ransomware-aanval. Verkoop, klantenservice en financiën werken niet meer. U bent een senior IT-leider die verantwoordelijk is voor het herstellen van de systemen, maar het vinden van een oplossing blijkt lastig te zijn.

Uw team, dat al onderbezet was, heeft wekenlang gewerkt met zeer weinig pauzes of vrije tijd. Sommige IT'ers hebben ***tot wel 36 uur achter elkaar gewerkt zonder te slapen.*** U maakt zich zorgen dat vermoeidheid leidt tot slechte besluitvorming, wat het herstel mogelijk in gevaar brengt.

U hebt dringend extra resources nodig die onmiddellijk kunnen helpen bij het oplossen van het probleem, maar waar u ze kunt vinden?

Dit scenario klinkt misschien als het begin van een roman, maar is gebaseerd op de echte ervaringen van Dell klanten. Het belicht een belangrijk probleem in de huidige cyberbeveiligingsomgeving: de menselijke factor.

Uit recente data blijkt dat de branche te kampen heeft met een tekort aan bijna 5 miljoen beveiligingsprofessionals. Hoewel de behoefte aan resources het meest acuut wordt gevoeld tijdens een incident, beginnen de oplossingen veel eerder in het proces.

Begin met het opbouwen en uitbreiden van een pipeline van talent

De eerste stap om ervoor te zorgen dat u over de resources beschikt die u nodig hebt, is het opbouwen van een pipeline van talent:

Werving van studenten en stageplaatsen

Door samen te werken met lokale universiteiten en technische scholen is er toegang tot een constante stroom van jong talent. Deze personen kunnen na verloop van tijd worden opgeleid tot waardevolle teamleden.

Voortdurende training en ontwikkeling

Hoewel tijd en budget constant onder druk staan, moeten cyberbeveiligingsprofessionals veranderingen in zowel tools als bedreigingen bijhouden.

Focus op retentie

Er is veel vraag naar goede IT'ers, vooral als ze ervaring hebben met het navigeren door een aanval. Als u uw toptalent niet behoudt, doet iemand anders dat.

Zelfs een sterk team is mogelijk niet voldoende om de stress die komt kijken bij het beheren van een aanval aan te kunnen, dus plan vooruit door extra support te identificeren voordat deze nodig is:

Evalueer bronnen van derden

Bedrijven voor cyberbeveiligingsadvies en personeelsuitbreiding kunnen uw team helpen tijdens lopende activiteiten en incidenten. Bouw relaties op met deze bedrijven, ook als u ze nu niet nodig hebt, zodat u toegang hebt tot die resources wanneer u ze wel nodig hebt.

Dell biedt een reeks diensten aan die bestaande teams kunnen versterken, waaronder een virtuele CISO (vCISO), incidentrespons en cyberbeveiligingsadvies.

Maak gebruik van AI

Profiteer van nieuwe AI-mogelijkheden die worden ingebouwd in cyberbeveiligingstools, zoals logboekanalyse, anomaliedetectie, triage van waarschuwingen op laag niveau of gespecialiseerde training om tekorten aan resources op te vangen en operationele behoeften aan te pakken, waardoor teamleden zich mogelijk kunnen richten op belangrijkere taken.

Uitdagingen in verband met resources zijn het grootst tijdens een cyberaanval

Zoals in het eerste scenario werd geïllustreerd, kan een grote cyberaanval uw organisatie verlammen, waardoor belangrijke systemen en bedrijfsactiviteiten worden lamgelegd. Elke minuut kost het bedrijf geld en het cyberbeveiligingsteam staat onder enorme druk om het probleem op te lossen.

Ervoor zorgen dat uw teams over de laatste kennis beschikken, heeft een directe impact op de incidentrespons en gerelateerde teamstress.

Houd er rekening mee dat training niet alleen bedoeld is voor de beveiligingsprofessionals, maar voor alle werknemers, omdat zij de eerste verdedigingslinie vormen.

Dit verhaal onderstreept een centrale uitdaging: de cyberverdedigers zijn uiteindelijk menselijk. Ze hebben grenzen, en wanneer deze grenzen worden overschreden, kunnen zelfs de sterkste professionals het opgeven. Geestelijke vermoeidheid, stress en burn-out zijn nu cruciale factoren in de cyberbeveiligingsmentaliteit.

Hoewel er misschien geen universele oplossing voor dit probleem is, kunnen de volgende strategieën een groot verschil maken:

Een sterk team samenstellen en een pipeline van talent opbouwen
De meest fundamentele oplossing voor dit probleem is om te voorkomen dat het een noodgeval wordt: stel een sterk team samen met redundanties.

Rekening houden met de menselijke kant van een aanval
Incidentresponsplannen zijn van cruciaal belang en ze MOETEN plannen omvatten voor het beheer van medewerkers, de planning en de omgang met uitval van werknemers.

Maak gebruik van resources van derden
Externe cyberbeveiligingsconsultants kunnen u helpen uw team uit te breiden. De incidentresponsservices van Dell zorgen er bijvoorbeeld voor dat er binnen enkele uren een deskundig team ter plaatse is, dat klaar is om het incident te beoordelen, te beperken en onmiddellijk te beginnen met het herstel. We hebben veel klanten geholpen om cyberaanvallen te doorstaan.

AI kan helpen, maar is geen wondermiddel

AI biedt een enorme belofte om cyberbeveiligingstools en -programma's te verbeteren. De mogelijkheden van AI zullen uiteindelijk uiteenlopen van voorspellende analyse tot het ontwikkelen van op maat gemaakte trainingsprogramma's en zelfs het proactief aanpakken van bedreigingen voordat ze zich verspreiden.

Misschien nog belangrijker is dat AI de verdedigers een realtime supportsysteem kan bieden tijdens een incident. Machine learning-modellen die zijn getraind op historische aanvalsdata kunnen acties aanbevelen op basis van vergelijkbare gebeurtenissen uit het verleden.

Naarmate natuurlijke taalverwerking wordt geïntegreerd in cyberbeveiligingstools, hebben analisten de mogelijkheid om rechtstreeks met hun systemen te communiceren, bedreigingen te identificeren en oplossingen te implementeren.

AI kan ook gedragspatronen bewaken om aan te geven wanneer een menselijke analist, mogelijk uit vermoeidheid, herhaaldelijk fouten maakt en vragen om deze te vervangen.

Hoewel cyberbeveiligingstools in hoog tempo geavanceerdere AI-tools integreren, zijn veel van de krachtigste mogelijkheden nog in ontwikkeling. Houd er rekening mee dat AI op dit moment nog niet de vaardigheden van een ervaren IT'er kan vervangen, ***vooral niet van iemand die al eens een aanval heeft*** meegemaakt.

Aanbevelingen om te profiteren van AI:

Ontdek hoe de tools uw beveiligingsactiviteiten kunnen helpen
Voer een gedetailleerde analyse uit van AI-tools en implementeer ze waar ze het meest effectief kunnen zijn. Mogelijke makkelijke successen zijn onder andere geavanceerde bedreigingsdetectie, het automatiseren van repetitieve taken en het gebruik van AI in identiteitsbeheer.

> Het is een aanbevolen procedure om een partner te hebben die incidentrespons en herstel uitvoert op basis van een retainer."
>
> ***Jason Rosselot***
> *VP, Cybersecurity and Business Unit Security Officer, Dell Technologies*

Plan voor de toekomst van AI
Begrijp wanneer nieuwe mogelijkheden beschikbaar komen, hoe ze uw team ten goede komen en ontwikkel een plan om ze te implementeren.

Integratie van AI in personeelsplanning
Naarmate automatisering handmatige taken vermindert, moet de samenstelling van uw beveiligingsteam mogelijk veranderen. Het kan zijn dat u resources op een hoger niveau nodig hebt om beveiligingsinformatie te analyseren en te verwerken, in plaats van deze te verzamelen. Pas uw wervings- en ontwikkelingsstrategieën dienovereenkomstig aan.

AI wordt een belangrijk onderdeel van uw cyberbeveiligingsactiviteiten, als dit nog niet het geval is. Maar houd er rekening mee dat een deskundige en ervaren IT'er onvervangbaar is. Het doel moet zijn om AI te gebruiken om activiteiten te automatiseren en medewerkers effectiever te maken, waardoor aanvallen uiteindelijk worden voorkomen en de impact ervan wordt geminimaliseerd wanneer ze zich voordoen.

Bevorder de volwassenheid van cyberbeveiliging: stap voor stap

Net als alles op het gebied van cyberbeveiliging is het aanpakken van het menselijke element een reis, geen bestemming. Incrementele inspanningen en zelfs kleine stappen richting vooruitgang maken een verschil en tellen na verloop van tijd op. Het is belangrijk om te onthouden dat zelfs de beste technologie en beveiligingstools uiteindelijk slechts zo goed zijn als de mensen die gebruik van ze maken.

DELL Technologies

Dell producten en oplossingen die u kunnen helpen

Aanbevolen Dell oplossing	Omschrijving
Services voor incidentrespons	Een team van door de branche gecertificeerde cyberbeveiligingsexperts staat klaar voor snelle respons in het geval van een cyberaanval. We werken samen met u om de bedreigingen te elimineren totdat de normale activiteiten zijn hervat.
Cybersecurity Advisory Services	Deskundige begeleiding die u kan helpen blinde vlekken in uw beveiligingsstrategie te vinden en aan te pakken, uw assets en data te beschermen en continue waakzaamheid en governance mogelijk te maken.
vCISO	Virtual Chief Information Security Officer en cyberbeveiligingsexpert die kan helpen bij het identificeren en beheren van risico's en het begeleiden van strategische besluitvorming.
Managed Detection and Response	Vermindert handmatige inspanningen en stroomlijnt dagelijkse beveiligingsactiviteiten door bewaking, bedreigingsdetectie, onderzoek en snelle respons te bieden op eindpunten, het netwerk en in de cloud. Klanten kunnen kiezen uit hun favoriete XDR-platform (Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR of Microsoft Defender XDR) en ontvangen deskundige begeleiding, driemaandelijkse rapporten en tot 40 jaarlijkse incidentresponsuren.

Ontdek hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van vandaag kunt aanpakken op **dell.com/cybersecuritymonth**