DELL Technologies

Kwaadwillende insider: versterking van cyberbeveiliging en veerkracht met Dell Technologies

De toenemende dreiging van kwaadwillende aanvallen van insiders

Kwaadwillende aanvallen van insiders zijn een van de meest urgente cyberbedreigingen in het huidige zakelijke landschap geworden. In tegenstelling tot externe bedreigingen beschikken kwaadwillende insiders al over een zekere mate van vertrouwen en toegang binnen een organisatie, waardoor hun acties bijzonder schadelijk en moeilijker te detecteren zijn. Aanvallen van insiders - van toegang tot gevoelige data tot sabotage van systemen - kunnen kritieke activiteiten verlammen en ernstige financiële en reputatieschade veroorzaken.

Dell Technologies erkent het groeiende gevaar van deze aanvallen en ontwikkelt innovatieve, schaalbare oplossingen om bedrijven in staat te stellen de risico's van kwaadwillende insiders te identificeren, te voorkomen en te beperken. Door state-of-the-art technologie te combineren met door experts geleide services, helpt Dell organisaties deze interne bedreigingen voor te blijven.

Wat zijn aanvallen van een kwaadwillende insider?

Een aanval van een kwaadwillende insider vindt plaats wanneer iemand binnen een organisatie zijn toegang misbruikt om gegevens te compromitteren, activiteiten te verstoren of gevoelige informatie te stelen voor persoonlijke, financiële of concurrentiedoeleinden. Deze persoon kan een werknemer, aannemer, partner of iemand met legitieme toegang tot de systemen en netwerken van het bedrijf zijn.

Hoe schadelijke aanvallen van binnenuit werken

Kwaadwillende insiders misbruiken hun vertrouwde positie om traditionele beveiligingsmaatregelen te omzeilen. Veelgebruikte technieken zijn onder meer:

1. **Datadiefstal:** stelen van vertrouwelijke klantdata, intellectueel eigendom of financiële data.
2. **Sabotage:** doelbewust schade toebrengen aan IT-systemen om bedrijfsactiviteiten te verstoren of de reputatie te schaden.
3. **Misbruik van inloggegevens:** gestolen of misbruikte inloggegevens gebruiken om de toegangsrechten te verhogen of dummy-accounts te maken.
4. **Samenwerking met externe aanvallers:** toegang of gevoelige kennis delen met externe cybercriminelen in ruil voor financieel gewin.

Dit dubbele voordeel van vertrouwen en interne kennis maakt kwaadwillende insiders bijzonder gevaarlijk in vergelijking met externe aanvallers.

De impact voor bedrijven

De gevolgen van kwaadwillende aanvallen door insiders zijn ingrijpend en ze veroorzaken niet alleen financiële schade. Bedrijven kunnen te maken krijgen met gevolgen zoals:

Financieel verlies

Diefstal van gevoelige informatie, fraude of sabotage leidt tot inkomstenverlies en herstelkosten die miljoenen dollars kunnen bedragen.

Operationele verstoring

Systeemsabotage of datavernietiging kan de activiteiten stopzetten, wat resulteert in vertragingen, gemiste kansen en verminderde productiviteit.

Reputatieschade

Een lek of aanval door een insider ondermijnt het vertrouwen van klanten en belanghebbenden, wat gevolgen heeft voor de loyaliteit van klanten en de marktperceptie.

Niet-naleving van wetgeving

Afhankelijk van de sector kunnen aanvallen van binnenuit leiden tot hoge boetes en straffen als gevoelige data uit de gezondheidszorg of financiële sector worden gebruikt.

Praktijkvoorbeeld

In 2020 heeft een IT-aannemer die voor een grote financiële instelling werkte, opzettelijk kritieke systeemconfiguraties verwijderd, waardoor er gedurende meer **dan 10 uur** netwerkstoringen werden veroorzaakt. Deze sabotage leidde tot **miljoenen** dollars aan financiële verliezen, uitgebreide herstelkosten en reputatieschade. Dergelijke incidenten illustreren het vernietigende potentieel van de dreiging van binnenuit en benadrukken de urgentie van robuuste detectie- en preventiemaatregelen.

83%

van de organisaties meldde het afgelopen jaar ten minste één aanval waarbij een insider was betrokken

Bron: 2024: Cybersecurity Insiders' Report

Geschatte kosten

Volgens een onderzoek van het Ponemon Institute uit 2024 worden de gemiddelde kosten van een incident waarbij een insider is betrokken, geschat op **$ 4,99 miljoen**, en vormen deze incidenten bijna **55%** van alle lekken. In dit cijfer is rekening gehouden met de kosten van detectie, herstel en inperking, waardoor duidelijk wordt hoe belangrijk het is dat organisaties investeren om de risico's van insiders preventief te beperken.

Bestrijding van schadelijke aanvallen van insiders met Dell Technologies

Dell Technologies biedt een uitgebreid ecosysteem van tools en services om schadelijke bedreigingen van insiders te bestrijden, zodat uw organisatie voorbereid is op het onverwachte.

Veilige eindpunten met Dell Trusted Devices

Eindpunten dienen vaak als toegangspunt voor bedreigingen van binnenuit. Dell Trusted Devices hebben geavanceerde beveiligingsfuncties in hun hardware om eindpunten te versterken en gevoelige data te beschermen.

- **Dell SafeBIOS** zorgt voor firmware-integriteit en voorkomt pogingen om systeembewerkingen op hardwareniveau te manipuleren.
- **SafeID** beschermt inloggegevens, waardoor ongeautoriseerde toegang en misbruik van inloggegevens wordt voorkomen.
- **SafeData** versleutelt gevoelige data end-to-end, zodat onderschepte of gestolen informatie onleesbaar blijft voor kwaadwillende insiders.

Door deze oplossingen te implementeren, kunnen organisaties ervoor zorgen dat hun eindpunten worden beschermd, ongeacht of de bedreiging intern of extern is ontstaan.

Proactieve bedreigingsdetectie met CrowdStrike

Het identificeren van bedreigingen van binnenuit vereist zichtbaarheid en bewaking van het gedrag van gebruikers. CrowdStrike, geïntegreerd in de oplossingen van Dell, maakt gebruik van kunstmatige intelligentie en gedragsanalyses om afwijkingen te detecteren die wijzen op bedreigingen van binnenuit.

Abnormale dataoverdracht buiten kantooruren of onbevoegde toegang tot kritieke gebieden van het netwerk worden bijvoorbeeld onmiddellijk gemarkeerd, waardoor een snelle respons mogelijk is. Een Amerikaanse gezondheidszorgorganisatie maakte onlangs gebruik van proactieve dreigingsdetectie om de poging van een werknemer om patiëntgegevens te stelen te identificeren en te beëindigen, waardoor een kostbaar lek werd voorkomen.

Verbeterde databescherming met Dell PowerProtect

Dell PowerProtect biedt een robuuste verdedigingslinie door middel van veilige back-ups, air-gapped storage en onveranderlijke kopieën van kritieke data. Door ervoor te zorgen dat gevoelige informatie wordt beschermd tegen wijziging of verwijdering, kunnen aanvallen van insiders die gericht zijn op data-integriteit worden voorkomen.

Een voorbeeld is een productiebedrijf dat te maken had met een ontevreden werknemer die ontwerpen probeerde te saboteren. Met de herstelkluis van Dell PowerProtect kon het bedrijf zijn activiteiten binnen enkele uren weer oppakken, verstoring voorkomen en de bedrijfscontinuïteit behouden.

Snel incidentherstel met Dell Professional Services

Wanneer een bedreiging van insiders escaleert in een incident, is snel herstel essentieel. Dell Professional Services, waaronder extern dataherstel en incidentrespons, zorgt ervoor dat bedrijven data en systemen snel kunnen herstellen. De experts van Dell leiden het proces, om downtime te minimaliseren en de gevolgen te beperken.

Dit zijn slechts een paar voorbeelden binnen het Dell portfolio van oplossingen die kunnen helpen bij kwaadwillende bedreigingen van insiders.

Geavanceerde netwerkbeveiliging en microsegmentatie met Dell PowerSwitch Networking en SmartFabric OS

Versterkt de bescherming tegen zero-day-aanvallen door geavanceerde netwerksegmentatie, strikte toegangscontroles en realtime verkeersanalyse te leveren in uw hele infrastructuur.

Het belang van een meerlaagse beveiligingsaanpak

Voor een effectieve verdediging tegen risico's van insiders is meer dan één beschermingslaag vereist. Het implementeren van een meerlaagse beveiligingsstrategie zorgt ervoor dat geen enkel beveiligingslek een zwak punt wordt. De belangrijke stappen zijn onder meer:

Belangrijke stappen om uw verdediging te verbeteren

- **Zero-Trust-principes:** verifieer voortdurend alle toegangsaanvragen en ga ervan uit dat geen enkele entiteit inherent vertrouwd is, ook niet binnen de perimeter.
- **Role-Based Access Controls (RBAC):** beperk de toegang van werknemers tot alléén de systemen en data die ze voor hun rol nodig hebben.
- **Geavanceerde versleutelingsoplossingen:** versleutel data in rust en onderweg, waardoor datadiefstal wordt geneutraliseerd.
- **Bewustwording en training van werknemers:** implementeer frequente bewustwordingsprogramma's ten aanzien van de beveiliging om te voorkomen dat werknemers per ongeluk deelnemen aan schadelijke activiteiten.
- **Regelmatige systeemtests:** voer penetratietests en beveiligingsscans uit om ervoor te zorgen dat uw verdediging betrouwbaar blijft.

Deze werkwijzen, ondersteund door de oplossingen van Dell, zorgen voor een stevig, holistisch beschermingsframework tegen kwaadwillende insiders.

Versterking van de verdediging door middel van strategische partnerschappen

Dell werkt samen met toonaangevende cyberbeveiligingsproviders, waaronder **CrowdStrike** en **Secureworks**, om hun oplossingen verder te versterken. CrowdStrike verbetert de beveiliging van eindpunten en biedt waardevolle informatie over bedreigingen op basis van compromisindicatoren, terwijl Secureworks geavanceerde bedreigingsdetectie- en responsservices biedt. Deze samenwerking zorgt ervoor dat klanten van Dell profiteren van een ecosysteem van geïntegreerde en geavanceerde technologieën.

Waarom Dell Technologies voor cyberbeveiliging de beste keuze is

Dell Technologies blijft bepalen wat de gouden standaard meerlaagse cyberbeveiligingsoplossingen is. Bedrijven profiteren van de toonaangevende expertise, verregaande partnerschappen en een innovatieve suite aan Dell producten die zich aanpassen aan het veranderende bedreigingslandschap van vandaag. Van eindpuntbeveiliging tot insiderdetectie tot incidentherstel, Dell biedt een compleet, veerkrachtig kader dat vertrouwen inspireert en groei mogelijk maakt.

Bouw aan een veerkrachtige toekomst met Dell Technologies

Bescherm uw bedrijf tegen schadelijke bedreigingen van binnenuit met de uitgebreide, schaalbare oplossingen van Dell Technologies. Door samen te werken met Dell beveiligt u niet alleen uw activiteiten, maar zorgt u ook voor bedrijfscontinuïteit, bevordert u het vertrouwen van klanten en maakt u uw organisatie toekomstbestendig. Neem contact met ons op voor meer informatie over het implementeren van een proactieve verdediging.

Dell Technologies is uw vertrouwde bondgenoot bij de bestrijding van bedreigingen van binnenuit, het beschermen van uw kritieke assets en het helpen van uw bedrijf om te bloeien in een dynamische digitale omgeving. Een toekomst van beveiliging is een toekomst van succes, en die begint bij Dell.

Ontdek op **Dell.com/SecuritySolutions** hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van dit moment kunt aanpakken

Meer informatie over Dell oplossingen

Neem contact op met een Dell Technologies expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag

DELL Technologies