DELL Technologies

Zero-day: Versterking van cyberbeveiliging en veerkracht met Dell Technologies

De toenemende dreiging van zero-day-aanvallen

Zero-day-aanvallen zijn in korte tijd uitgegroeid tot een van de grootste uitdagingen in het huidige cyberbeveiligingslandschap. Deze aanvallen maken misbruik van beveiligingslekken die onbekend zijn bij de softwareleveranciers en beveiligingsexperts, waardoor bedrijven onvoorbereid en kwetsbaar zijn. Organisaties in alle sectoren, van de gezondheidszorg tot de financiële sector, zijn kwetsbaar voor dergelijke inbreuken, die vaak ernstige financiële en operationele gevolgen hebben.

Het tempo van de digitale transformatie versnelt en zero-day-aanvallen komen steeds vaker voor en worden steeds geavanceerder. De behoefte aan robuuste beschermingsmaatregelen is nog nooit zo groot geweest. Dell Technologies begrijpt het kritieke karakter van deze bedreiging en biedt bedrijven innovatieve, schaalbare verdedigingsmechanismen om zero-day-aanvallen effectief te bestrijden en te herstellen.

Wat zijn zero-day-aanvallen?

Een zero day-aanval houdt in dat misbruik wordt gemaakt van een niet bekendgemaakte beveiligingslek in software of hardware voordat er een patch of oplossing beschikbaar is. Aanvallers profiteren van de kans die zich voordoet en veroorzaken vaak grootschalige verstoringen voordat de kwetsbaarheid wordt ontdekt en verholpen.

Hoe zero-day-aanvallen werken

1. **Detectie van kwetsbaarheden:** Hackers identificeren coderingsfouten of verborgen achterdeurtjes in softwareapplicaties of -systemen.
2. **Ontwikkeling van exploits:** Malware wordt gemaakt om misbruik te maken van het beveiligingslek. Aanvallers kunnen gerichte phishingcampagnes of websites met malware gebruiken om de exploit te leveren.
3. **Uitvoering van een aanval:** De exploit wordt ingezet, waardoor het systeem in gevaar wordt gebracht en mogelijk gegevensdiefstal of operationele interferentie mogelijk is.

Veelvoorkomende technieken

- Drive-by Downloads zetten gebruikers ertoe aan om onbewust malware te installeren.
- Phishing-e-mails verspreiden kwaadaardige links of payloads om kwetsbaarheden te misbruiken.
- Bestandsloze aanvallen omzeilen detectie door operaties volledig in het geheugen van een systeem uit te voeren.

Deze zeer geavanceerde aanvalsvectoren maken zero-day-aanvallen bijzonder gevaarlijk, omdat traditionele op handtekeningen gebaseerde detectietools ze vaak niet herkennen.

De impact op bedrijven

Zero-day-aanvallen brengen aanzienlijke risico's met zich mee vanwege hun onvoorspelbaarheid en de vertraging bij de detectie ervan. De gevolgen kunnen op verschillende fronten rampzalig zijn.

Financieel verlies

Een succesvolle zero-day-aanval kan hoge kosten met zich meebrengen, van boetes van toezichthouders tot inkomstenverlies tijdens downtime. Een niet-geïdentificeerd beveiligingslek dat in een e-commerceplatform wordt misbruikt, kan bijvoorbeeld het afrekenproces onmogelijk maken, wat direct van invloed is op de verkoop.

Gevolgen voor de reputatie

De publieke perceptie van een bedrijf kan onherstelbaar worden geschaad. Klanten verliezen hun vertrouwen wanneer gevoelige informatie openbaar wordt gemaakt of diensten niet werken.

Operationele storing

Onopgeloste kwetsbaarheden leggen systemen vaak lam, wat leidt tot een daling van de productiviteit, vertraagde projecten en gemiste zakelijke kansen.

Praktijkvoorbeeld

Een grote zorgaanbieder werd het slachtoffer van een zero-day-aanval die gericht was op niet-gepatchte software voor medische apparatuur. De aanval verstoorde belangrijke activiteiten, legde patiëntgegevens bloot en kostte de organisatie **miljoenen** aan herstelkosten, terwijl het vertrouwen van patiënten werd aangetast.

Alarmerende statistieken

Onderzoek wijst uit dat volgens een Ponemon-studie uit 2023 ongeveer 80% van de inbreuken betrekking heeft op zero-day

Zero-day-aanvallen vertegenwoordigen consistent meer dan **70%** van de misbruikte kwetsbaarheden

Bron: 2024: IMandiant "M-Trends"

Zero-day-aanvallen bestrijden met Dell Technologies

Dell Technologies levert toonaangevende oplossingen waarmee bedrijven zich actief kunnen beschermen tegen zero-day-aanvallen en snel kunnen herstellen na dergelijke inbreuken.

Beveiligingsoplossingen voor servers en storage

De server- en storagebeveiligingsoplossingen van Dell bieden extra beschermingslagen:

- Beveiligde servers controleren en blokkeren pogingen tot ongeautoriseerde toegang.
- Back-up- en herstelsystemen voor data zorgen ervoor dat zelfs in het ergste geval kritieke informatie toegankelijk en intact blijft.

Versterkte eindpunten met Dell Trusted Devices

Eindpunten zijn een belangrijk toegangspunt voor aanvallers. Dell Trusted Devices bevatten geavanceerde beveiligingsmaatregelen, zodat eindpunten beschermd blijven tegen onbekende bedreigingen.

- **SafeBIOS** beschermt firmware tegen manipulatie en waarborgt zo de integriteit van het systeem vanaf de basis.
- **SafeID** beschermt gebruikersreferenties door verificatieprocessen te beveiligen.
- **SafeData** versleutelt gevoelige data in rust en onderweg, waardoor deze onbruikbaar wordt in het geval van onderschepping of misbruik.

Proactieve bedreigingsdetectie met CrowdStrike

CrowdStrike maakt gebruik van geavanceerde analytics en AI om de activiteit van eindpunten te bewaken en ongebruikelijk gedrag te detecteren dat kan duiden op zero-day-aanvallen. De proactieve bedreigingsdetectie zorgt voor snelle respons voordat beveiligingslekken kunnen leiden tot wijdverbreide schade.

Een telecommunicatieprovider die CrowdStrike gebruikt, kon bijvoorbeeld afwijkingen in het netwerkverkeer vroegtijdig detecteren, waardoor een potentieel zero-day-misbruik op de servers van de klant werd beperkt.

Dell PowerProtect oplossingen

Dell PowerProtect biedt robuuste, onveranderlijke back-ups en geïsoleerde herstelopties. Bedrijven kunnen hun activiteiten snel en efficiënt herstellen na een zero-day-aanval, waardoor de bedrijfscontinuïteit behouden blijft en essentiële klantdata worden beschermd.

Een grote winkelketen bijvoorbeeld gebruikte PowerProtect om versleutelde bestanden te herstellen die waren gecompromitteerd door een ransomware-aanval als gevolg van een zero-day-kwetsbaarheid, waardoor langdurige downtime werd voorkomen.

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

Echte beveiliging vereist meer dan één oplossing. Een meerlaagse strategie combineert technologie, processen en mensen om een uitgebreid beschermingsframework te vormen.

Belangrijke acties om defensie te versterken

- **Gebruik Zero-Trust-principes:** Controleer elk individu en apparaat dat toegang probeert te krijgen tot het netwerk.
- **Geavanceerde versleuteling implementeren:** Gebruik versleutelingsprotocollen om zowel bewegende als inactieve data te beschermen.
- **Informeer werknemers:** Bied gedetailleerde trainingssessies om werknemers te leren phishing-pogingen en social engineering-tactieken te herkennen.
- **Systemen regelmatig testen:** Voer consistente penetratietests en beveiligingsscans uit om ervoor te zorgen dat de verdediging zich aanpast aan nieuwe bedreigingen.

Dell Technologies koppelt deze praktijken aan de geavanceerde beveiligingsoplossingen, zodat organisaties klaar zijn om zero-day-kwetsbaarheden effectief te bestrijden.

Partnerschappen die cyberbeveiliging versterken

De samenwerking van Dell met marktleiders **Microsoft**, **CrowdStrike** en **Secureworks** biedt klanten toegang tot geavanceerde beveiligingsintelligentie en -tools.

- **Microsoft** integreert naadloos met Dell oplossingen om systeembrede compatibiliteit en proactieve beschermingsmechanismen te garanderen
- **CrowdStrike** biedt geavanceerde informatie over eindpuntbedreigingen om potentiële zero-day-exploits te detecteren.
- **Secureworks** biedt voortdurende controle en deskundige probleemoplossing voor realtime aanvallen.

Dell Professional Services gebruiken

De Professional Services van Dell bieden een uitgebreid scala aan advies, implementatie en herstelondersteuning om bedrijven te helpen bij het aanpakken en beperken van de risico's die gepaard gaan met zero-day-bedreigingen. Van incidentrespons tot roadmap-planning voor cyberbeveiliging, Dell helpt organisaties om veerkracht op de lange termijn te bereiken.

Een veerkrachtige toekomst bouwen

Investeren in Dell Technologies betekent een partner hebben die niet alleen superieure technologie, maar ook gemoedsrust biedt. Met geavanceerde oplossingen, strategische partnerschappen en ongeëvenaarde expertise stelt Dell organisaties in staat om zelfs de meest geavanceerde zero-day-aanvallen te anticiperen, te detecteren en te herstellen.

Neem vandaag nog contact op met Dell Technologies om uw bedrijf te beveiligen, uw reputatie te beschermen en te groeien in een onvoorspelbaar digitaal landschap. Vertrouw op Dell om uw toekomst te versterken tegen de bedreigingen van morgen.

Dell Technologies wekt vertrouwen en stelt bedrijven in staat om de uitdagingen van zero-day-aanvallen een stap voor te blijven dankzij haar beveiligingsoplossingen en -diensten die zijn ontworpen om te beschermen wat het belangrijkst is.

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

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