Dell beveiligingspraktijken voor apparaten

Drie overwegingen voor het instellen van vertrouwen in apparaten

Cyberexperts van Dell leggen uit welke cruciale rol de beveiligingspraktijken van apparaten spelen in de tolerantie van uw IT-ecosysteem op de lange termijn.

Auteurs
Rick Martinez
Dell Fellow en Vice President

Eric Baize
VP, Product- en applicatiebeveiliging

Inleiding

In de drukke cybermarkt van vandaag zit u waarschijnlijk overspoeld met opties voor beveiligingsproducten en -oplossingen. Maar wat als ik u vertelde dat het belangrijkste onderdeel van uw beveiligingsstrategie niet uw beveiligingsproducten zijn?

Als grote pc-fabrikant denkt Dell veel aan beveiliging. En wat in de afgelopen jaren duidelijk is geworden terwijl we de verwoestende gevolgen van ransomware-aanvallen en de uitbreiding van firmware-gebaseerde malware zien, is dat eindpuntapparaten een groeiend doelwit zijn. Helaas kunnen éénpuntoplossingen, hoe innovatief ook, gebruikers en data niet volledig veilig houden.

Naarmate u uw bestaande ecosysteembeveiliging opnieuw beoordeelt en producten verkent voor een refresh, overweeg dan hoe uw pc-fabrikant de beveiliging benadert en wat u moet kopen. Waarom? U denkt misschien dat het gaat om productevaluatie, maar het gaat evenzeer om leveranciersevaluatie. Een vertrouwde en ervaren leverancier van veilige pc's die het bedreigingslandschap begrijpt, kan die kennis gebruiken om u te helpen uw organisatie te beschermen naarmate dat landschap zich ontwikkelt. Met die partner bouwt u een beveiligingsecosysteem dat de onvermijdelijke aanval op intelligente wijze beperkt en cybertolerantie op de lange termijn stimuleert.

Beveiliging begint eerder dan u denkt

IT-besluitvormers en eindgebruikers hebben doorgaans te maken met een mix van verkoopmedewerkers, apparaten en productondersteuning. Maar dat is nog maar het topje van de ijsberg als het gaat om beveiliging. Waarom? Het is vergelijkbaar met voedselveiligheid. U kunt voedselveiligheid niet alleen beoordelen op basis van uw interacties met een ober in een restaurant. Voedselveiligheid begint namelijk in de keuken. Ook wat apparaten veilig maakt, moet aanwezig zijn, zelfs voordat een product wordt geproduceerd. Dit is daardoor zelden zichtbaar. Dell heeft talloze technische uren en intellectuele inspanningen besteed aan het beveiligen van de IT-werkomgeving van de klant vanaf de basis: de ingewikkelde processen en protocollen die het ontwerp,

de ontwikkeling en de levering van elk apparaat regelen. Het werk dat niemand ziet en wat de stabiele basis vormt onder het oppervlak om het veiligste apparaat mogelijk te maken. Het werk dat helpt de IT-werkomgeving van de klant te beveiligen, of u nu een federale klant, onderneming of een klein en middelgroot bedrijf bent. Dell gelooft in het mogelijk maken van moderne beveiliging voor alle bedrijven, groot en klein. We zetten ons dan ook in om oplossingen te leveren die uw organisatie en bij uitbreiding uw klanten veilig houden.

Onze praktijken voor apparaatbeveiliging

Wanneer we kijken naar de bescherming van onze commerciële apparaten, denken we aan de beveiligingsresultaten, d.w.z. hoe het apparaat bijdraagt aan de algehele beveiligingsstatus van een organisatie. Hoe helpt het apparaat aanvallen te voorkomen? Wat houdt het veilig tijdens een aanval? En hoe blijft het gedurende de hele levensduur veilig?

Zoals u misschien verwacht, beschikken we over tientallen methoden voor het ontwikkelen van veilige zakelijke pc's die zijn afgestemd op de industriestandaarden en een Zero Trust-beveiligingsaanpak ondersteunen. Vandaag breng ik enkele kernthema's onder de aandacht: een beveiligde leveringsketen, beveiligde code en beveiliging in gebruik.

1. We beveiligen onze leveringsketen van apparaten. Dat betekent strikte controles rond onze leveringsketens voor zowel hardware als software, oftewel de fysieke en digitale leveringsketens. Deze controles helpen de kwaliteit van onze producten te waarborgen tijdens het productie-, assemblage- en leveringsproces, en tot aan de implementatie. Dit zorgt ervoor dat onze klanten precies krijgen wat ze hebben gekocht, niets meer en niets minder. Bovendien geven we deze strikte vereisten door aan al onze leveranciers. Dat gezegd hebbende, in de echte Zero Trust-modus 'aanname van inbreuk' nemen we verificatiecontroles op tijdens elke stap van dit proces.

Deze controles omvatten geavanceerde technologieën zoals Secured Component Verification* om componentwisselingen te identificeren en SafeBIOS off-host verificatie om eventuele sabotage van de meest gevoelige firmware in het systeem te identificeren en te waarschuwen. Deze en vele andere functies zijn ingebouwd in Dell Trusted Devices, onderdeel van ons Dell Trusted Workspace portfolio. Maar we maken er ook gebruik van in onze hele leveringsketen om alle schakels in de keten intact te houden. Hierdoor kunnen we afwijkingen detecteren voordat ze de volgende stap van de leveringsketen bereiken. (*Optionele add-on-functie beschikbaar voor aankoop. Beschikbaarheid verschilt per regio.)

Dat is wat ik bedoel met resultaatgericht zijn. Deze functies zijn ontwikkeld niet omwille van innovatie, maar omdat ze actief echte zorgen oplossen die onze klanten hebben met betrekking tot de beveiliging van de leveringsketen en het beheer van het wagenpark. Vertrouw nooit, verifieer altijd.

Onthoud dat bij het evalueren van leveranciers de leveringsketen van uw OEM uw eigen leveringsketen is. Zorg er dus voor dat u de praktijken die zij hanteren grondig onderzoekt. (Zie onze whitepaper over de leveringsketen voor meer inzicht in wat er nodig is om de leveringsketen te beveiligen.)

2. We ontwerpen en ontwikkelen veilige apparaten. Hier ziet u waar de praktijk en functies elkaar kruisen. Zo ontwikkelen we effectieve en innovatieve hardware en firmware.

Beveiligingsfuncties maken nu deel uit van ons marktgerichte aanbod, maar dat is slechts een deel van de puzzel. Onze producten zouden niet veilig zijn als het ontwerp, de ontwikkeling en de tests niet worden beheerst door onze prescriptieve Secure Development Lifecycle (SDL). Een kernverantwoordelijkheid van alle technologieleveranciers is ervoor te zorgen dat wat ze verkopen niet onbedoeld een risico vormt voor gebruikers via van kwetsbaarheden. Om aanvallen te voorkomen en veerkracht te bieden aan onze beveiligingssoftwarestack, voeren we rigoureuze bedreigingsmodellering uit tijdens het softwareontwikkelingsproces. Daarnaast identificeren we risico's aan de hand van zeer geavanceerde aannames van tegenstanders en passen we deze methodiek zelfs toe op kritieke hardware.

We testen en verifiëren de aannames van deze bedreigingsmodellen tijdens het hele ontwikkelingsproces, waarbij we samenwerken met enkele van de beste consultants voor tests voor indringingsrisico en externe onderzoekers, die proberen Dell systemen te doorbreken. Op dezelfde manier bieden we een openbaar bug bounty-programma om de beveiliging van onze zakelijke pc's te testen. We gebruiken de uitkomsten van deze rapporten als informatie voor de technische afdeling om maatregelen te ontwikkelen. Herhalen en herhalen. Waarom doen we dit? De omgevingen van onze klanten vereisen robuuste en vertrouwde apparaten om effectief te kunnen werken.

3. We werken eraan om ervoor te zorgen dat apparaten veilig in gebruik zijn. Bij beveiliging komt van alles kijken. En tegenwoordig omvat echte beveiliging bescherming op hardware- en firmwareniveau, evenals software. Daarom doet Dell enorme inspanningen om een ecosysteem van volledig gescreende, toonaangevende partners te creëren die bescherming bieden tegen geavanceerde bedreigingen. Veel zijn rechtstreeks geïntegreerd in onze zakelijke pc's. Maar hackers innoveren voortdurend nieuwe manieren om in software te breken. Daarom zijn onze SDL-praktijken ontworpen om de bescherming na de release uit te breiden, inclusief de mogelijkheid om kwetsbaarheden snel en eenvoudig te identificeren en op te lossen. Dell rapporteert ook proactief aanstaande beveiligingsupdates en duidelijke beleidsregels voor beveiligingssupport om het voor klanten gemakkelijker te maken om te begrijpen hoe hun producten gedurende hun hele levensduur beschermd blijven. Om klanten te helpen snel informatie te vinden over kwetsbaarheden en toepasbaarheid voor productreleases, hebben we alle beveiligingsadviezen en -kennisgevingen op één plek geconsolideerd. Door dit te combineren met een goed gedocumenteerd responsbeleid voor kwetsbaarheden, kunnen we nauw samenwerken met onderzoekers wanneer nieuwe kwetsbaarheden worden gemeld. Dit maakt de lus kleiner en zorgt ervoor dat altijd nauwkeurige informatie beschikbaar is, zodat klanten risico's binnen hun omgeving kunnen beoordelen en herstellen.

Een beveiligingspartner die alles samenbrengt

Dell streeft naar vertrouwen en een veilige, verbonden wereld. Wij werken zonder ophouden om de data, het netwerk, de organisatie en de veiligheid van u en uw klanten te garanderen, met beveiliging die zorgvuldig is ingebouwd in al onze oplossingen. Ga voor meer informatie over onze beveiligingspraktijken naar het Dell Security and Trust Center. U kunt altijd contact opnemen met uw Dell vertegenwoordiger met vragen of met onze beveiligingsspecialisten via global.security.sales@dell.com

Meer informatie over Dell Endpoint Security

Neem contact op met een Dell Technologies expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag

DELL Technologies