ActualTech Media

Hewlett Packard Enterprise

# HPE biedt ingebouwde beveiliging voor het mkb

Ed Tittel

## INHOUDSOPGAVE



## IN DEZE PAPER

HPE biedt ingebouwde beveiliging die zich uitstrekt van het siliciumniveau tot in de toeleveringsketen van de server om bescherming te bieden gedurende de gehele IT-levenscyclus. In dit technische overzicht wordt onderzocht hoe HPE de beveiliging direct en expliciet aanpakt via verschillende mechanismen.

Beveiliging speelt een rol in alle aspecten van de IT-operaties in de hele organisatie. Beveiliging is dus niet alleen belangrijk voor systeemhardware en -software, maar ook voor de mensen die dergelijke zaken gebruiken. Het opzetten en onderhouden van beveiliging werkt het beste voor bedrijven die een leverancier kiezen die begrijpt dat beveiliging in systemen en software moet worden ontworpen, vanaf het begin moet worden ingebouwd en moet worden onderhouden als onderdeel van een volledig levenscyclusproces. HPE biedt zelfs volledige beveiligingsdekking voor het hele bedrijf, van begin tot eind, voor alle systemen en gebruikers.

## Wat beveiliging betekent in 2021

Een goede algemene definitie van cyberbeveiliging is het geheel van technologieën, processen en werkwijzen die zijn ontworpen en toegepast om digitale systemen en activa, inclusief netwerken, apparaten, software en gegevens, te beschermen tegen aanvallen, schade of verlies en ongeoorloofde toegang. Beveiliging is dus van nature alomvattend en heeft betrekking op systemen, communicatie, programma's, data en verbindingen. Gevoelige gegevens vereisen vaak bijzondere aandacht en bescherming, of het nu gaat om intellectuele eigendom, financiële gegevens, persoonlijk identificeerbare informatie (PII), medische dossiers of andere soorten gegevens. Als dit aan de verkeerde partijen bekendgemaakt wordt, kan dat negatieve gevolgen hebben, zowel voor de organisatie die dergelijke data bezit als voor de partij waarnaar de gegevens verwijzen of die ze toebehoort.

Beveiliging wordt vaak toegepast op specifieke aandachtspunten of zorgen en omvat doorgaans:

- **Serverbeveiliging:** De verzameling tools, technologieën, instellingen, firmware en software (zowel binnen als buiten het besturingssysteem van de server) waarmee de beveiliging van netwerkservers van een organisatie wordt gedefinieerd en verzorgd. Vaak gaat het om toegang tot infrastructuurbeveiligingselementen, evenals serverfirmware en op zichzelf staande onderdelen en softwareonderdelen van het besturingssysteem.
- **Clientbeveiliging:** De verzameling tools, technologieën, instellingen, firmware en software (zowel binnen als buiten het besturingssysteem van de client) waarmee de beveiliging van netwerkclients van of die gerelateerd zijn aan een organisatie wordt gedefinieerd en verzorgd. Wordt vaak gezien als synoniem voor eindpuntbeveiliging omdat clients in de meeste organisaties het grootste deel van de eindpunten uitmaken. Bevat gewoonlijk onderdelen voor het opsporen en voorkomen van bedreigingen, waaronder antimalware, patch- en updatebeheer en meer. Werkt ook samen met infrastructuurbeveiligingselementen, zowel lokaal als op afstand (indien van toepassing).
- **Netwerkbeveiliging:** De verzameling tools, technologieën, apparaten en software die zich op netwerkapparaten bevinden of deze bewaken en beheren (zowel fysiek als virtueel). Houdt over het algemeen inspectie en filtering van netwerkverkeer in, voornamelijk aan netwerkgrenzen om in- en uitgaand verkeer te controleren. Kan infrastructuurbeveiligingselementen hosten, vaak in de vorm van softwaregedefinieerde netwerken (SDN) voor lokale of wide-area (SD-WAN) netwerkonderdelen en -services.
- **Cloudbeveiliging:** De verzameling tools, technologieën en software die zich bevindt in, toezicht houdt op en het beheer uitvoert van de toegang en het gebruik van de cloud, de configuratie en provisioning, demontage en buitenbedrijfstelling en het bewaken van verkeer/activiteiten. Cloudbeveiliging is bedoeld om de onderliggende fysieke infrastructuur te beschermen, maar kan zich ook uitstrekken tot virtuele infrastructuren en services die in de cloud worden uitgevoerd en data die in de cloud worden gebruikt.
- **Beveiliging van de infrastructuur:** De verzameling tools, technologieën en software die gebruikt worden voor het bewaken en beheren van alle onderdelen van de netwerken en infrastructuur van een organisatie, met inbegrip van client-, server- en netwerkapparaten, evenals cloudonderdelen en -services die toegankelijk zijn voor de organisatie. Infrastructuurbeveiliging biedt een totaalbeeld van volledige infrastructuren, via dashboards, automatisering en andere tools die gebruikt worden om de samenstellende elementen en componenten te bekijken, te beheren en te controleren.

> **HPE kan kleine bedrijven helpen om te gaan met al deze beveiligingspunten en -zorgen, en ervoor zorgen dat hun strategieën voor risicomanagement in overeenstemming zijn met hun zakelijke doelen en doelstellingen.**

Interessant is dat cyberbeveiliging al deze verschillende aandachtspunten en zorgen omvat. Het gaat om software, hardware en firmware die gebruikt worden op clients, servers en netwerken die direct onder controle van een organisatie staan. Het gaat ook om cloudgebaseerde onderdelen die vaak door derden worden beheerd (vaak een cloudplatform, -services of Software-as-a-Service [SaaS]-provider met een publieke of private cloud).

> **Silicon root of trust voorkomt dat beschadigde firmwarecode wordt uitgevoerd.**

Risicobeheerservices spelen ook in op cyberbeveiliging omdat ze zich bezighouden met het verminderen of elimineren van risicobronnen die mogelijk de inkomsten, het vermogen om zaken te doen of de reputatie van een organisatie kunnen schaden door middel van defensieve of beschermende maatregelen. Het vereist het prioriteren en beheren van digitale verdedigingsmiddelen om de mogelijke negatieve gevolgen van de bedreigingen die ze vormen te compenseren (kleine of minder grote risico's krijgen weinig of geen respons, terwijl grote of enorme risico's een grote en substantiële respons krijgen). HPE kan kleine bedrijven helpen om te gaan met al deze beveiligingspunten en -zorgen, en ervoor zorgen dat hun strategieën voor risicomanagement in overeenstemming zijn met hun zakelijke doelen en doelstellingen. In de volgende paragrafen worden specifieke HPE technologieën toegelicht die gebruikt worden om specifieke beveiligingsrisico's te compenseren, met name voor HPE servers en de bijbehorende clients.

## Silicon Root of Trust

Silicon root of trust is ontworpen om bescherming te bieden tegen specifieke, gerichte firmware- en BIOS-aanvallen. Het werkt voor HPE ProLiant-servers en brengt een koppeling tot stand tussen aangepaste HPE silicium op die servers en de bijbehorende Integrated Lights Out (iLO)-firmware. In wezen voorkomt silicon root of trust dat beschadigde firmwarecode wordt uitgevoerd. Dit gebeurt door het uitvoeren van integriteitscontroles op firmwarecode voordat deze mag worden uitgevoerd, met behulp van speciale, alleen-lezen controlesommen en vergelijkingstools die niet direct toegankelijk zijn voor het besturingssysteem of programma's die bovenop het besturingssysteem worden uitgevoerd.

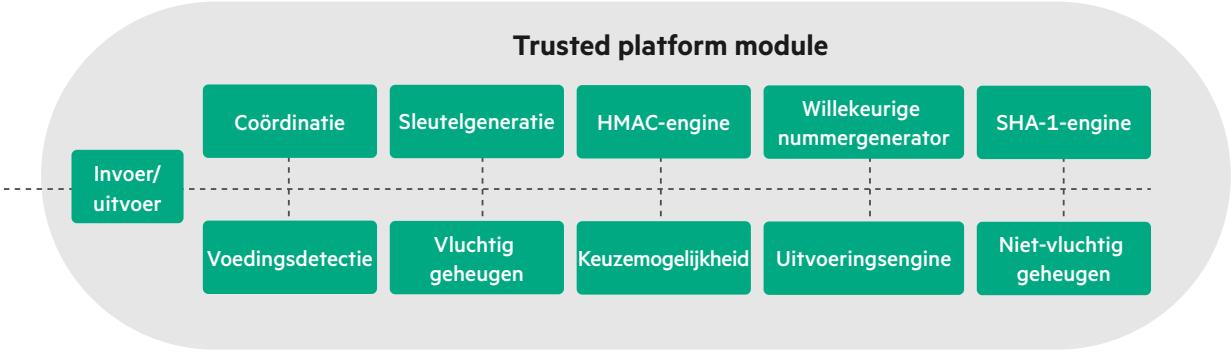
Wanneer er aanwijzingen van manipulatie of wijzigingen worden gedetecteerd, verwijdert de HPE iLO-firmware de mogelijk (of daadwerkelijk) beschadigde firmwarecode. De gevonden code wordt vervangen door een geldige, bekende en correcte firmware-image van een betrouwbare bron. Vervolgens wordt die bekende, goed werkende kopie automatisch uitgevoerd. HPE iLO integreert versleuteling met zijn tools voor het detecteren van inbreuken, zodat alleen veilige firmwarecode kan worden uitgevoerd. Als een dergelijke veilige firmwarecode niet kan worden opgehaald of uitgevoerd, zal de server worden uitgeschakeld en wordt er geen mogelijk beschadigde firmware uitgevoerd. Dit zorgt ervoor dat HPE ProLiant-servers beschermd worden tegen rootkits en andere aanvalsmethoden en -vectoren voorafgaand aan het opstarten.

### HPE Pointnext Security Services

HPE Pointnext Services is de ondersteunende, adviserende, professionele en educatieve serviceorganisatie van HPE. HPE experts werken samen met klanten van HPE om hen te helpen uitdagingen op het gebied van beveiliging en risicobeheer aan te pakken binnen hun IT-activiteiten op het gebied van de digitale transformatie van edge tot cloud. HPE werkt graag samen met middelgrote en kleine bedrijven om hen te helpen hun medewerkers voor te bereiden en hun werknemers om te scholen met beveiligingstrainingen en certificeringen. Digital Learner-abonnementen bundelen de technische HPE training voor gebruik door mkb-teams en combineren toegang tot alle waarde in training die HPE biedt, tegen een betere prijs.

## Trusted Platform Module (TPM)

De TPM heeft de vorm van een computerchip (microcontroller) die veilig artefacten opslaat die gebruikt worden om een runtime-platform te verifiëren, inclusief servers en client-pc's (laptops, tablets, all-in-ones enzovoort). Sinds januari 2021 vereist Microsoft dat alle nieuwe Windows Server-platforms TPM-versie 2.0 bevatten, met Secure Boot standaard ingeschakeld, en beveelt aan dat alle servers ook BitLocker-versleuteling gebruiken voor extra bescherming tegen mogelijke “rootkit”-malware-aanvallen. HPE ondersteunt TPM sinds het in 2009 een ISO/IEC-standaard (11990) werd. Tegenwoordig voldoen alle beschikbare moderne HPE ProLiant-servers en pc's van HP, Inc. aan deze vereisten of overtreffen ze deze.




**Afbeelding 1:** De Trusted Platform Module biedt beveiligde, op chips gebaseerde storage-, verwerkings- en versleutelingstools voor gebruik tijdens het opstarten

Zoals te zien is in **afbeelding 1** biedt een TPM een beveiligde omgeving waar veilige referenties zoals sleutels, certificaten, wachtwoorden enzovoort veilig gegenereerd, opgeslagen en gebruikt kunnen worden buiten de normale verwerkingsomgeving van het apparaat. De TPM is ontworpen om zeer fraudebestendig en veilig te zijn, en om een op silicium gebaseerde vertrouwensbasis te bieden om te beschermen tegen rootkit-, firmware- en andere aanvalsvectoren voorafgaand aan het opstarten.

Op een pc (server of client) biedt een TPM veilige opslag voor beheerderstoegang en BIOS-updates. Het ondersteunt ook versleuteling op schijfniveau (bijv. Microsoft BitLocker), biometrische gegevens (bijv. gezichtsherkenning of vingerafdrukinformatie van Microsoft Windows Hello) en de veilige opstartfaciliteit van Microsoft. Een TPM maakt dus een op hardware gebaseerde beveiliging op laag niveau tegen aanvallen op laag niveau mogelijk en ondersteunt deze. Microsoft werkt samen met alle grote chipleveranciers (AMD, intel en Qualcomm) om te zorgen voor een goede integratie van TPM-functionaliteit op CPU-niveau. De moderne servers van HPE en de client-pc's van HP, Inc. ondersteunen allemaal minimaal TPM 2.0 en bieden gebruikers en organisaties een solide, beschermde vertrouwensbasis van silicium.

> De moderne servers van HPE en de client-pc's van HP, Inc. ondersteunen allemaal minimaal TPM 2.0 en bieden gebruikers en organisaties een solide, beschermde vertrouwensbasis van silicium.

## HPE's vertrouwde toeleveringsketen

Om klanten met bovennormale beveiligingseisen en zeer veilige gebruiksscenario's van dienst te zijn, werkt HPE met een vertrouwde toeleveringsketen. Onder gebruikers van deze toeleveringsketen vallen consumenten in de federale en publieke sector van de Verenigde Staten die enkel producten uit de Verenigde Staten met verifieerbare cybergarantie mogen aanschaffen. Kopers van buiten de Verenigde Staten kunnen via deze vertrouwde toeleveringsketen over de hele wereld aankopen doen (met uitzondering van China, Taiwan en India). Beveiliging is op twee specifieke manieren direct ingebouwd in deze vertrouwde toeleveringsketen. Ten eerste wordt deze gerealiseerd door middel van extra geharde beveiligingskenmerken in de producten zelf. Ten tweede wordt deze gecontroleerd door HPE medewerkers die tijdens het productieproces toezicht houden op deze producten. HPE medewerkers controleren alle onderdelen, observeren de assemblage en zorgen ervoor dat de verpakte apparaten vrij van manipulatie blijven totdat de klant de levering accepteert.

Daarnaast omvat HPE een exclusieve siliconen root of trust die beveiliging op basis van siliconen in standaard servers inbouwt en beveiligingscontroles in de volledige toeleveringsketen handhaaft om strenge beveiliging op hardwareniveau te garanderen. De verhardingstechnieken van HPE omvatten UEFI Secure Boot, een kleiner aanvalsoppervlak, bestendigheid tegen sabotage op siliciumniveau, geïntegreerde alarmen in systemen en fysieke vergrendelingen.

Bezoek de pagina HPE beveiligingsoplossingen voor meer informatie over de ingebouwde end-to-end-beveiliging van HPE via onder meer de vertrouwensbasis van silicium, TPM en de mogelijkheden van de vertrouwde toeleveringsketen.