Bij installatie start cyber security ellende

Veel cyber security ellende begint vaak al bij het installeren van een besturingssysteem. Het is o zo gemakkelijk om de CD in een computer te stoppen en 'next', 'next', 'next' te klikken. Natuurlijk slaagt de installatie en zal de computer starten. Hoera! Goed gedaan. Maar het is de vraag of daarmee alle basisvoorzieningen zijn getroffen om te komen tot een veilig systeem. De meeste fabrikanten van besturingssystemen zetten, om begrijpelijke redenen, alles wagenwijd open. Gebruikers willen per slot van rekening zonder problemen alle software kunnen installeren. Cybercriminelen maken hier handig gebruik van. Bijvoorbeeld door via een virus of phishing e-mail een nieuwe, schoon geïnstalleerde computer te voorzien van kwaadaardige software.

Hardening Als men het installeren van een besturingssysteem goed wil doen, zal hardening een vast onderdeel moeten zijn van het installatieproces. Hardening is het proces waarbij door middel van het parametriseren van de (technische) configuraties en de instellingen systemen en/of netwerken veiliger worden.
Een goed hardeningproces omvat servers, actieve netwerkcomponenten zoals firewalls en switches, desktops, laptops en mobiele devices. Hardening gebeurt door overbodige functies in besturingssystemen en hard- en software uit te schakelen en/of te verwijderen. Doordat bij hardening zodanige waarden worden toegekend aan specifieke parameters wordt de mogelijkheid voor kwaadwillenden om een systeem te compromitteren sterk verlaagd, gaat de veiligheid omhoog en krijgt kwaadaardige software geen kans.
Een voorbeeld voor de noodzaak van hardening is dat na nieuwe installatie van Windows op een computer automatisch zaken als bureauaccessoires of Windows Mediaspeler zijn meegeïnstalleerd. Ze zijn niet nodig, maar wel geïnstalleerd en veroorzaken dus een mogelijk risico ten aanzien van de systeembeveiliging. Maar ook zaken zoals het uitschakelen van autorun, het invoeren van een wachtwoordpolicy op het systeem en het beperken van informatie die op open poorten wordt weggegeven verhogen de systeemveiligheid. Het kan ook gaan om het verwijderen van niet gebruikte of onnodige gebruikersaccounts. Ook het wijzigen van standaard wachtwoorden, die op sommige systemen aanwezig kunnen zijn, is onderdeel van het hardeningproces en draagt bij aan een betere beveiliging.
Vraag blijft, wat moeten we wel en niet uitschakelen en/of verwijderen? Om hierin duidelijkheid te brengen, geven organisaties zoals het Center for Internet Security (CIS) zogenaamde Benchmarks uit. Deze zijn waardevolle documenten die kunnen helpen met de parametrisering van systemen en applicaties benodigd voor het hardeningproces.

Arbeidsintensief De hardening van besturingssysteem en applicaties is een arbeidsintensief proces. Immers, parameter na parameter moet worden bekeken, ingesteld en getest. Vaak gaat het om honderden parameters. Daarnaast is hardening een momentopname, want het installeren of deïnstalleren van bijvoorbeeld

'De meeste fabrikanten van besturingssystemen zetten alles wagenwijd open. Cybercriminelen maken hier handig gebruik van.'

applicatiesoftware kan een net geparametriseerd (gehardend) besturingssysteem volledig overhoop gooien. Vooral bij deïnstalleren gebeurt het nogal eens dat parameters niet goed worden teruggezet, waardoor risico's ten aanzien van de beveiliging kunnen ontstaan. Het is dus ook aan te bevelen om periodiek de harding van systemen te controleren. Natuurlijk kan dit handmatig, maar dit is kwalitatief sterk afhankelijk van de uitvoerder van het proces. Het is dan ook beter om periodiek geautomatiseerd de status van de hardening in kaart te brengen. Fabrikanten zoals Easy2Audit, Lumension en Siemens leveren hiervoor geautomatiseerd scanners waarmee de status van de hardening eenvoudig in kaart kan worden gebracht. De scanners bevragen het systeem, zonder software of iets dergelijks te installeren. De resultaten van deze bevraging worden verzameld in een file en vervolgens verwerkt tot een rapportage.
Hardening is een belangrijk proces bij het inrichten van een computer, maar wordt vaak vergeten. Het handmatig uitvoeren van hardening is arbeidsintensief, maar kan veel cyber security ellende voorkomen. Het is belangrijk hardening vast onderdeel te maken van het installatieproces en afscheid te nemen van de 'next, next, next, hoera!'-klikkers.

Ronald Eygendaal schrijft regelmatig over informatiebeveiliging, elektronische en technische beveiliging, fraudedetectie en -bestrijding, bewaking en beveiliging. Hij is bestuurslid bij de VBN.