Cyber security ellende begint bij installatie

Systeem hardening

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. Maar of alle basisvoorzieningen dan getroffen zijn om tot een veilig systeem te komen, is maar de vraag. De meeste fabrikanten van besturingssystemen zetten immers, om begrijpelijke redenen, alles wagenwijd open. Gebruikers willen per slot van rekening zonder problemen alle software kunnen installeren. Cybercriminelen maken hier handig gebruik van, door bijvoorbeeld via een virus of phishing e-mail uw nieuwe mooi geïnstalleerde computer te voorzien van kwaadaardige software.

Als men het installeren van een besturingssysteem goed wil doen dan 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 hardeningsproces omvat servers, actieve netwerkcomponenten, zoals firewalls en switches, desktops, laptops en mobiele devices. Kortom hardening bestrijkt de volledige keten van automatiseringssystemen en netwerken. Hardening gebeurt door overbodige functies in besturingssystemen en hard & software uit te schakelen en/of te verwijderen. Doordat bij hardening zodanige waarden worden toegekend aan specifieke parameters wordt de mogelijkheid om een systeem te compromitteren sterk verlaagd, gaat de veiligheid omhoog en krijgt kwaadaardige software geen kans.

Een voorbeeld van de noodzaak van hardening is, dat na nieuwe installatie van Windows op een computer automatisch zaken als bureau-accessoires of Windows Mediaspeler zijn mee geïnstalleerd. Ze zijn niet nodig, maar wel mee geïnstalleerd en veroorzaken dus een mogelijk risico ten aanzien van de systeembeveiliging. Maar ook zaken zoals het uitschakelen van autorun, het invoeren van een wachtwoord policy op het systeem, het beperken van informatie die op open poorten wordt weggeven en dergelijke meer verhogen de systeemveiligheid. Denk niet alleen aan Windows systemen, zo kan men bij bijvoorbeeld Unix systemen denken aan het verwijderen of uitschakelen van onnodige services zoals X11 of de Telnet daemon. Maar 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 hardening proces en dragen bij aan een betere beveiliging.

CIS Security Benchmarks

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 CIS Security Benchmarks zijn waardevolle

documenten die kunnen helpen met de parametrisering van systemen en applicaties nodig voor het hardeningsproces. Naast het CIS geven overheden, banken en andere ICT grootgebruikers hun eigen hardeningsrichtlijnen uit.
Tevens geven veel fabrikanten van besturingssystemen en hard en software documenten uit waarin ze aangeven hoe hun producten kunnen worden gehardend.

Arbeidsintensief proces

De hardening van een besturingssysteem en applicaties is een arbeidsintensief proces. Parameter na parameter moet immers worden bekeken, worden ingesteld en worden getest. Vaak gaat het om honderden parameters. Daarnaast is hardening een momentopname, want het installeren of de-installeren van bijvoorbeeld applicatiesoftware kan een net geparametriseerd (gehardend) besturingssysteem volledig overhoop gooien. Vooral bij de-installeren 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 de harding van systemen periodiek te controleren. Natuurlijk kan dit handmatig. Zoals echter reeds eerder aangegeven is dit zeer arbeidsintensief en is het kwalitatief sterk afhankelijk van de uitvoerder van dit proces.
Het is dan ook beter om periodiek geautomatiseerd de status van de hardening in kaart te brengen. Fabrikanten zoals Easy-2Audit, 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. Vaak bevatten de scanners uitgebreide rapportage mogelijkheden zodat organisaties naar auditors en toezichthouders kunnen aantonen "in control" te zijn.

Conclusie

Hardening is een belangrijk proces bij het inrichten van een computer, wat vaak wordt vergeten. Het handmatig uitvoeren van hardening is een arbeidsintensief proces, maar het kan veel cyber security ellende voorkomen. Het is dus belangrijk hardening vast onderdeel te maken van het installatieproces en afscheid te nemen van de next, next, next hoera klikkers….

(Door Ronald Eygendaal)

Bronnen:

- **http://www.cisecurity.org/resources-publications/**
- **http://www.easy2audit.com/**
- **https://www.lumension.com/kb/Home/Endpoint-Security/874.aspx**