De mythe van veilig offline computergebruik

21 juli 2017 Artikel

Als we veilig willen werken, dan houden we onze computers offline. Het is maar de vraag of die schijnzekerheid ook door de hoofden speelde bij al die IT-professionals, betrokken bij de autofabrikant Renault, de Britse NHS-ziekenhuizen, de parkeerbeheerder QPark en de Duitse spoorwegen. Wat we wel weten is dat ransomware 'WannaCry' waarschijnlijk tienduizenden computers heeft geïnfecteerd in meer dan 100 landen.

Cyberaanvallen op grote schaal voltrokken zich tot dusver voornamelijk via het e-mailverkeer met virussen, verstopt in de aangehechte bestanden van e-mailberichten. WannaCry richtte zich niet tot de PC's van individuele gebruikers. De ransomware infecteerde onder meer kaartjesautomaten en digitale dienstregelingen. Er is dus een ander aanvalsplan gevolgd, waaraan wellicht toch een fout van een individuele computergebruiker ten grondslag ligt. Iemand heeft bijvoorbeeld een geïnfecteerde website bezocht. Virussen op websites gedragen zich anders dan hun pendanten in het e-mailverkeer. Browsers en zeker browser plug-ins hebben zwakke plekken waarlangs een infectie zich kan verspreiden.

Echt verraderlijk is het scenario wanneer er helemaal geen individueel computergebruik aan te pas komt. Bijna elk modern computersysteem, groot en klein, werkt met processen en services op de achtergrond. Indien een aanvaller erin slaagt die processen te voeden met gemanipuleerde data, heeft hij in principe toegang tot de andere delen van het computersysteem. De controle over de computer laat zich volledig overnemen. Wanneer deze is aangesloten op een netwerk, heeft de aanvaller zich toegang verschaft tot het netwerk. In complexe software, zoals bijvoorbeeld operating systems (OS) zijn altijd dergelijke zwakheden te ontdekken. Er bestaan specialisten in het opsporen van die zwakke plekken. Zij brengen de software ontwikkelaars daarvan op de hoogte en gunnen hen de tijd met een tussentijdse oplossing (patch) te komen. Pas na verloop van tijd verneemt het grote publiek iets over het probleem en de voorhanden patch.

Kennis zwakheden voor hoogste bieder

Kwaadwillende onderzoekers van zwakke plekken verkopen hun bevindingen aan de hoogste bieder. Dit blijkt een bloeiende business te zijn. De software ontwikkelaar weet van niks, terwijl een selecte groep 'ingewijden' hun kennis ruimschoots kan misbruiken. In het geval van algemeen bekende zwakheden zijn gebruikers in de gelegenheid hun besturingssystemen tijdig te beschermen door het aanbrengen van de beveiliging updates. Maar dat moeten ze dan ook echt doen en er niet alleen over praten.

De vraag is terecht of we ons door het offline gebruik van computers wel kunnen afschermen tegen cyberaanvallen, want in een ’connected world’ zijn individuele systemen zelden altijd helemaal offline. Er zijn altijd momenten waarop software een functionele update ondergaat. Een onderhoudsmedewerker zal op de een of andere manier toegang moeten hebben tot bepaalde delen van de softwarecode. Zelfs in een omgeving met de hoogste beveiligingsclassificatie, zoals bij een nucleaire elektriciteitscentrale, werken servicetechnici geregeld aan de programmatuur van de besturings- en controlesystemen. Waar halen zij hun updates vandaan? Lopen zij nog rond met CD’s, gebrand vanaf verschillende computersystemen? Zelfs al zouden ze de gewenste code handmatig intikken, dan nog is er geen zekerheid, wanneer je niet weet of er achter die ingevoerde instructieregels geen virus schuil gaat.

Alleen selectief online gaan

Selectief online gaan op een gecontroleerde manier: ligt daarin de oplossing? Via een zware firewall alleen verbindingen toestaan met bekende systemen die de computer in de nucleaire elektriciteitscentrale nodig heeft om zichzelf te reorganiseren. Maar in hoeverre zijn die update servers te vertrouwen? De tijd, nodig voor het grondig controleren van die systemen en de toegangspoorten, zou wel eens ten koste kunnen gaan van de snelheid waarmee het betreffende computersysteem een update moet ondergaan. Des te langer je daarmee wacht, des te kwetsbaarder het systeem. De oude stelregel van veilig updaten gaat nog steeds op: zo min mogelijk en zoveel als noodzakelijk.

LVD, een Belgische fabrikant van metaalbewerkingsmachines, beveiligt het geavanceerde besturingssysteem met CodeMeter

Cyber security gericht op het beveiligen van de poorten van computersystemen moet, maar beveiligen vanuit het ontwerp van een systeem is beter. Terug naar de basis dus met het afschermen van de software tegen ongeoorloofd gebruik en ongewenste aanpassingen via een adequate licentieregistratie. En dan kan je daarna beslissen of je de software gratis ter beschikking stelt of juist niet. Het gaat allereerst om het effectief beveiligen van kwetsbare besturingssystemen.

Veel moderne besturingssystemen van vitale toepassingen binnen industriële omgevingen en nutsvoorzieningen (water, gas en elektriciteit) zijn gebaseerd op standaard hardware met standaard operating software als VxWorks, QNX, Windows of Linux Embedded. Ook in de Run-time omgevingen wordt vaak een gedeelde standaard toegepast, bijvoorbeeld CODESYS. Een fysieke scheiding van besturingssystemen en de apparaten of de productiemachines levert geen extra bescherming op. Vanuit hun laptops hebben servicemonteurs toegang tot controllers. De back ups van software en data, alsmede de instellingparameters zijn elders opgeslagen. Ze komen allemaal tezamen in de processor van het embedded computersysteem of de procescontroller (PLC). Dat is de plek waar de beveiliging cruciaal is. De controllers bevatten alleen uitvoerbare (run) code, waarvoor de configuratiegegevens en de parameters zijn vrijgegeven door daartoe gemachtigde functionarissen. De meest besturingsmodules zijn op locatie op te waarderen met nieuwe functionaliteit, terwijl gelijktijdig tijdens die sessie ’bugs’ zijn te ’fixen’. Als een onderhoudsspecialist toegang heeft tot software, kan een hacker er ook bij. Via een secure boot is misbruik te voorkomen.

Cryptografische versleuteling en digitale handtekeningen

Bij deze beveiligde opstartprocedure starten alle systeemonderdelen, inclusief de bootloader, vanuit een cryptografisch beveiligde omgeving die de betrouwbaarheid waarborgt. De afzonderlijke onderdelen van het besturingssysteem zijn voorzien van digitale handtekeningen van de producent en de technische manager van het productiebedrijf dat de PLC’s toepast. In het controleproces verifieert elke laag in het systeem of de volgende mag worden opgestart. De bootloader controleert het OS, dat op zijn buurt de

run-time omgeving controleert, waarna van daaruit de applicaties inspectie ondergaan (applicatie runtime, applicatie configuratie data).

In deze controleketen is het van belang dat de publieke sleutel van de eerste laag geen verandering ondergaat. Daarmee is de beveiliging van de gehele keten verankerd. Een pre bootloader in de vorm van een ’systemonchip’ (SOC) of een Trusted Platform Module (TPM) is waarschijnlijk het meest optimaal. Minder kostbaar is het toepassen van een tweevoudige bootloader, waarvan het deel met het initiële laadprogramma niet is te wijzigen. Aanvullende beveiligingsvoorzieningen zorgen ervoor dat een laag nagaat of de bewerking in de vorige laag correct is verlopen. De controle moet beide kanten op kunnen gaan. Voor de teruggaande controle volstaat een dongle met een usb-connector, (micro)SD-kaart of CF-kaart. Op dit externe, goed afgesloten blokje elektronica, is een zogeheten ’state machine’ aangebracht, die met een daarmee corresponderende versleutelde code de status van het opstartproces registreert. De ontcijfering voor het opstarten van de volgende laag vindt alleen dan plaats, wanneer is vastgesteld dat het voorgaande proces correct is verlopen en de status op de dongle is vastgelegd. De diverse software onderdelen laten zich dus nooit afzonderlijk en in samenhang door hackers simuleren.

Door het opnemen van een script met hash codes tussen de instructieregels, is met zekerheid vast te stellen of bepaalde programma’s nog dezelfde kenmerken hebben als toen ze voor het eerst werden geactiveerd. In de industriële wereld is het heel gebruikelijk om door middel van encryptie via hash codes en handtekeningcertificaten de verschillende lagen te controleren. De meeste moderne besturingssystemen voor ’embedded’ applicaties hebben de mogelijkheid om op het niveau van de ’bootloader’ de integriteit van het OS te laten checken alvorens deze te activeren.

Marcel Hartgerink, directeur Wibu-Systems Benelux

offline computergebruik, Wibu Systems