MET PATCHEN KUN JE NIET WINNEN; WEL VERLIEZEN

Ir. Dennis Baaten is information security officer bij de ANWB en bereikbaar via dbaaten@anwb.nl

Het tijdig installeren van updates (het zogenaamde 'patchen') is van cruciaal belang voor de informatiebeveiliging van een organisatie. Het aantal berichtgevingen in de media over kwetsbaarheden en het misbruik ervan, zorgt terecht voor de nodige verontrusting binnen en buiten de ICT-afdeling. Toch zorgen spanningsvelden in een organisatie ervoor dat het doorvoeren van patches niet zonder slag of stoot gaat. Overvolle agenda's bij beheerders, de eeuwige strijd om capaciteit en prioriteit, en een business die het patchen eerder als last dan als baat ervaart. Gelukkig hoef je hier niet in te berusten, maar kun je er ook iets aan doen.

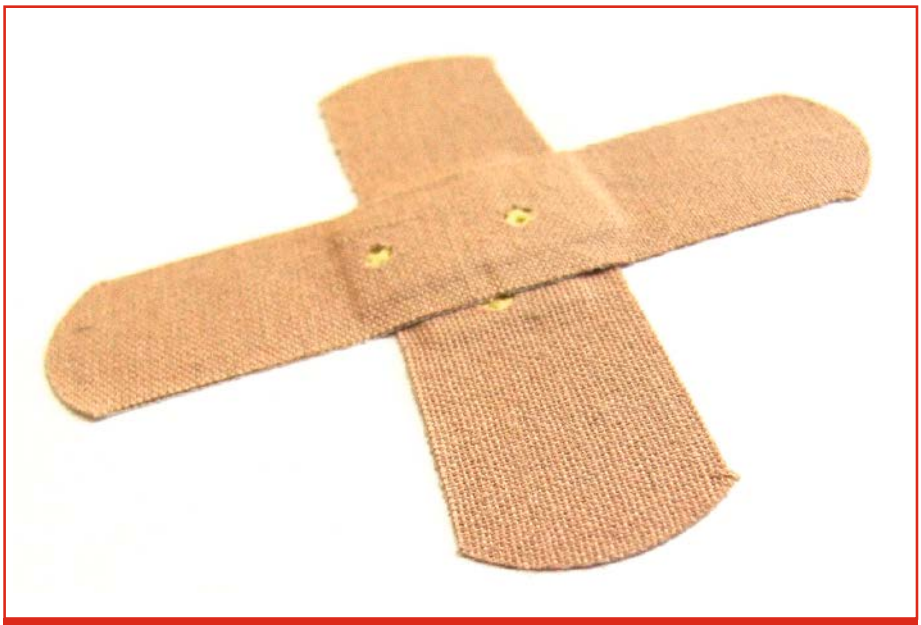
Het ICT-landschap van grote multidisciplinaire organisaties kent doorgaans een hoge complexiteit. Door de constante druk vanuit de business die de concurrentie een stapje voor wil blijven, volgen veranderingen en vernieuwingen elkaar in hoog tempo op. Tegelijkertijd blijft het ICT-budget dalen en lijkt 'meer voor minder' een door de crisis ingegeven noodzakelijke trend. De agenda's van de ICT-specialisten zitten vol met projecten waardoor er voor beheerwerkzaamheden (te) weinig tijd overblijft. Terwijl juist het beheer ervoor zorgt dat het ICT-landschap naar tevredenheid en met acceptabele risico's blijft functioneren.

Het overgrote deel van alle informatiebeveiligingsincidenten vindt plaats als gevolg van misbruik van kwetsbaarheden in verouderde software. Door het installeren van updates worden de gaten in de beveiliging verholpen en verdwijnt het risico op misbruik. Dit risico kan echter nooit tot nul teruggebracht worden, omdat patchen een reactief proces is. Je blijft afhankelijk van de snelheid waarmee een leverancier in staat is om patches voor ontdekte kwetsbaarheden uit te brengen. Hackers maken daarom in toenemende mate gebruik van zero-day-exploits om gaten in software te misbruiken voordat de leverancier van de software op de hoogte is van de kwetsbaarheid. Wanneer de leverancier dagen of weken na het geconstateerde misbruik een patch beschikbaar stelt, is het aan de eigen organisatie om patches snel uit te rollen. Hoe langer je wacht met updaten, des te groter de kans op misbruik. Maar het realiseren van een korte doorlooptijd voor organisatiebreed uitrollen van patches, blijkt vaak niet eenvoudig.

Patch achterstand oorzaak groot deel informatiebeveiligingsincidenten

Focus op het verkeerde risico

Veel organisaties hebben een standaard patchproces dat start bij het beschikbaar komen van een patch. De eerste stap is vaak het bepalen



van de prioriteit van de patch in termen van maximale doorlooptijd waarbinnen een patch uitgerold dient te zijn. Dit gebeurt op basis van (objectieve) externe bronnen en eigen kennis van het ICT-landschap, en is vaak vastgelegd in een beleidsdocument. De resulterende prioriteit kan worden gezien als een weerspiegeling van het risico dat de business bereid is te lopen. Na prioritering wordt de patch verpakt in een installatiescript en wordt de uitrol ervan getest. Bij een succesvolle test wordt het patchpakket (de daadwerkelijke patch + het installatiescript) organisatiebreed uitgerold. Op papier klinkt dat eenvoudig, maar de praktijk is helaas weerbarstiger.

In de praktijk heb ik inmiddels de nodige vertragende factoren de revue zien passeren. Zo komt het voor dat er teveel tijd nodig is om het patchpakket goed werkend te krijgen, maar heb ik ook gezien dat het testtraject te lang duurt doordat er onvoldoende capaciteit en middelen beschikbaar zijn om in korte tijd een representatieve test uit te voeren. Het is echter niet alleen de ICT-afdeling waar de vertragende factoren vandaan komen. Ook de business zorgt voor vertragingen, omdat men bijvoorbeeld niet altijd goed lijkt te begrijpen waarom een patch nodig is. En als je dat combineert met het feit dat de business niet altijd evenveel vertrouwen heeft in de ICT-afdeling, dan snap je wellicht ook waarom soms de hakken in het zand gaan.

Rol vrijgekomen beveiligingsupdates snel uit!

Dergelijke vertrouwenskwesties tussen de business en ICT zijn niet ongebruikelijk. Vaak worden ze veroorzaakt door ontevredenheid over de geleverde diensten en/of de moeizame procesgang die daaraan vooraf gaat. Bij patchen loopt het vertrouwen een deuk op wanneer er te vaak verstoringen worden veroorzaakt als gevolg van fouten tijdens het uitrollen. Vanuit de gedachte "hoe minder patches, hoe kleiner de kans dat er iets misgaat", probeert de business het uitrollen van patches tegen te houden om meer verstoringen te voorkomen. Een begrijpelijke emotie, maar vaak ligt hier niet de juiste afweging aan ten grondslag. De business focust in zo'n situatie teveel op het risico van verstoringen als gevolg van een foutieve patch, en verliest hierbij het oorspronkelijke risico uit het oog. En dat is het risico op misbruik als gevolg van een kwetsbaarheid.

Onzekerheid over bijeffecten patches leiden vaak tot uitstel

Je springt niet hoger door de lat te verlagen

De uitvoerende teams die binnen de ICT-afdelingen verantwoordelijk zijn voor het uitrollen van patches, worden continu met dit gebrek aan vertrouwen geconfronteerd. En doordat er ook de nodige druk ligt om patches snel door te voeren, komen de teams in een tweestrijd terecht. Het is of toegeven aan de druk vanuit de business om niet te patchen, of toegeven aan de druk vanuit het management om (vanuit het belang van informatiebeveiliging) wel te patchen. En omdat druk altijd de makkelijkste weg naar buiten zoekt, barst intern de discussie los aan het bureau van de information security officer.

Met name in de periodes waarin er in korte tijd veel kritieke patches uitkomen, houdt het patchen de gemoederen flink bezig. Van managers tot beheerders, velen stellen het huidige beleid ten aanzien van de prioritering van patches ter discussie. Er wordt sterk aangestuurd op het verhogen van de maximale doorlooptijd voor patches, maar dat is vanuit informatiebeveiliging zelden een goed idee. Niet omdat het zo leuk is om collega's te dwarsbomen, maar omdat een versoepeling van de norm niet de oplossing is voor dit probleem. Daarmee zou je alleen maar risico's introduceren waarvan de organisatie heeft aangegeven deze niet te willen lopen.

Verkorten van de doorlooptijd

De oplossing tot lage doorlooptijden is gelegen in een goede samenwerking tussen verschillende teams (dus

inclusief de business) vanuit een gemeenschappelijke doelstelling: een functionerend ICT-landschap met acceptabele risico's. Dat klinkt misschien cliché maar daarom, zoals wel vaker het geval met clichés, niet minder waar. Hieronder een aantal tips die je kunt toepassen:

1. *Inrichten van operationeel patchproces* – Richt het patchproces binnen de ICT-afdeling fatsoenlijk in. Zorg dat er voldoende capaciteit en prioriteit is voor het test- en uitrolteam. Vaak is dit een interne aangelegenheid en hoeft de business slechts geïnformeerd te worden.
2. *Leer van je fouten en kijk vooruit* – Fouten maken is niet erg, maar zorg er wel voor dat het er niet teveel zijn en leer ervan. Blijf zo min mogelijk in het verleden hangen en geef elkaar vertrouwen om het opnieuw te proberen. Anders is een poging om het over de inhoud eens te worden bij voorbaat gedoemd te mislukken.
3. *Hanteer een gefaseerde uitrol* – Rol niet uitsluitend uit met een big-bang, maar zorg voor een gefaseerde aanpak waarbij het risico op organisatie brede verstoringen wordt verkleind. Zorg dus voor voldoende mogelijkheden om patches gespreid uit te rollen, zodat de impact van onvoorziene verstoringen kan worden beperkt.

Gefaseerd uitrollen beperkt de patchrisico's

4. *Focus op de risico's* – Zorg dat iedereen begrijpt waarom het belangrijk is dat patches tijdig worden geïnstalleerd. Leg uit welke risico's er zijn, en benadruk dat risico's niet zomaar door specifieke afdelingen kunnen worden geaccepteerd, omdat misbruik van kwetsbaarheden de gehele organisatie treft.
5. *Spreek vaste onderhoudsvensters af* – Plan voldoende momenten in om patches en andere onderhoudswerkzaamheden uit te voeren. Maak met elkaar afspraken over hoe je omgaat met belangrijke patches buiten de vaste onderhoudsvensters.

Patchen is geen rocket science, maar een samenspel waar iedereen zich aan een vastgestelde set met spelregels dient te houden. Bovenstaande tips kunnen helpen de doorlooptijd te verlagen en daarmee het risico verkleinen. Snel en adequaat reageren op een kwetsbaarheid door te patchen vrijwaart je niet van computerinbraken, maar rekent wel grotendeels af met hackers die gaan voor het laag hangende fruit. En dat zijn er veel, heel veel. ●