Veilig en BYOD: incompatible?

Als de IT-beheerder(s) de hardware op een netwerk onder controle hebben, is het al moeilijk genoeg om de IT-omgeving te beveiligen, maar een Bring Your Own Device (BYOD) programma kan die uitdaging nog veel groter maken.

Wanneer een organisatie zijn medewerkers toestaat, hun eigen apparaten te gebruiken om bedrijfskritische gegevens en applicaties te benutten, moet er een BYOD beveiligingsstrategie zijn geformuleerd – en geïmplementeerd.

Malware

Een beleid dat BYOD en BYOPC (Bring Your Own PC) toestaat, kan een heel palet aan beveiligingsdreigingen opleveren. Private apparatuur kan malware – schadelijke software, virussen en dergelijke – in bedrijfsnetwerken implanteren. Vertrouwelijke of zelfs bedrijfskritische informatie kan op smartphones worden gedownload die vervolgens worden gestolen of kwijt raken. Een strategisch plan of klantgegegevens kunnen worden gestreamed van een server naar de tablet van een leidinggevende die met een zakenrelatie ergens in een restaurant zit; handig, maar niet als dat via een onbeveiligde verbinding plaatsvindt.

Om de voordelen van BYOD ten volle te benutten, zoals flexibiliteit en kostenbesparingen, moeten de gegevens die op de tablets, smartphones en andere apparatuur van de medewerkers zelf, adequaat worden beveiligd. Tevens moeten die gegevens 'onderweg' van en naar die apparaten worden afgeschermd. Maar als eerste dient een soort reglement te worden opgesteld waarin basisregels worden gegeven voor BYOD-beveiliging – en dat reglement moet ook worden nageleefd en gehandhaafd.

We geven hier enkele strategieën en tools voor het beheren van de databeveiliging en het garanderen van de naleving van de regels voor de werkomgeving met BYOD en BYOPC.

Beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid

Gegevensbeveiliging omvat grofweg drie soorten van beveiliging: vertrouwelijkheid, integriteit en beschikbaarheid. Als bedrijfsgegevens worden gekopieerd naar privé-apparatuur, mag geen van die drie soorten worden gecompromitteerd.

Het beschermen van vertrouwelijke gegevens heeft betrekking op het voorkomen van datalekken. Een effectief BYOD-beleid zorgt ervoor dat in de reglementen een dataklassificatie systeem is opgenomen waarin de totale gegevens'voorraad' is verdeeld in categorieën. Deze geven aan in hoeverre gegevens gekopieerd mogen worden op privé-apparatuur, bijvoorbeeld Categorie 1: geheel vrij; Categorie 2: beperkt door autorisatie; Categorie 3: niet. Voorbeelden van Categorie 3 zijn onder andere nieuwe productontwerpen of zaken die vallen onder de noemer intellectueel eigendom. Het kan best acceptabel zijn dat een medewerker een bepaalde hoeveelheid gegevens over klanten of andere zakelijke relaties op zijn of haar eigen tablet heeft staan, maar die medewerker moet dan wel op elk moment kunnen aantonen dat er een plausibele reden is waarom hij/zij die gegevens daarop heeft staan. Dat klinkt als Big Brother, maar het gaat tenslotte om het eigendom van het bedrijf.

Blokkeren

Dankzij de gemakkelijke manier en tools om gegevens te kopiëren (naar usb-stick, laptop of smartphone) kunnen zeer grote bestanden snel worden overgezet. Het is daarom raadzaam om in een BYOPC zogeheten 'data loss prevention' applicaties toe te passen: deze blokkeren de transfer van grote hoeveelheden vertrouwelijke informatie. Als kleinere hoeveelheden daarvan op privé-apparatuur wordt opgeslagen, is het risico weliswaar kleiner, maar niet geheel geëlimineerd.
De beperkingen op de hoeveelheid gegevens die mag worden gekopieerd, is afhankelijk van de rollen en verantwoordelijkheden van de respectievelijke personen. Die hebben dus allen een autorisatieniveau ontvangen van de IT-afdeling (als het goed is). Een medewerker Sales heeft redelijkerwijs informatie nodig over de klanten in zijn of haar rayon. Een marketinganalist heeft behoefte aan de gegevens van talloze, misschien wel alle klanten, maar heeft niets aan zeer gedetailleerde gegevens over al die klanten.

Fysieke beveiliging

Het BYOD-beleid moet ook rekening houden met fysieke beveiliging. Privé-apparaten waar bedrijfsgegevens op staan moeten beveiligd zijn tegen diefstal. En het moet niet te gemakkelijk worden gemaakt om grote hoeveelheden gegevens 'mee te nemen': het gebruik van usb-sticks voor het opslaan van bedrijfsgegevens is dus verboden.

Verloren of gestolen apparatuur is een groot probleem. In het beleid kan worden opgenomen dat er altijd een wachtwoord of ander inlogsysteem (bijvoorbeeld vingerafdruk) nodig is om een apparaat te openen. Maak ook gebruik van beheersystemen waarmee gestolen of verloren mobiele apparatuur op afstand kan worden 'gewiped'. Vanaf 1 juli 2015 is het in de Amerikaanse staat Minnesota zelfs verboden om smartphones te verkopen die geen zogenoemde 'kill switch' hebben. Privé-laptops en andere mobiele apparaten moeten encryptiesystemen hebben om het risico van een datalek te verkleinen als deze worden verloren of gestolen.

Bescherm de integriteit van de gegevens door de kans kleiner te maken dat er mee gerommeld wordt. Het instellen van een wachtwoord of een andere beveiliging tegen ongeoorloofd openen, is dan slechts de eerste stap. Smartphones en laptops zouden altijd beveiligd moeten zijn met een wachtwoord. Die wachtwoorden zijn persoonlijk, dus houd ze dan ook persoonlijk: zet ze niet op een geel plakbriefje dat rondslingert. De truc om het naar jezelf te mailen en dat mailtje dan op te slaan in de map Bewaren werkt natuurlijk niet. Zeker niet als de werkplek met iemand anders gedeeld wordt. Iedere gebruiker moet zijn eigen account hebben, en dus zijn eigen wachtwoord, om de gegevens die hij nodig heeft voor zijn taken en waar hij voor geautoriseerd is, te kunnen openen en bewerken.

'BESCHERM DE INTEGRITEIT VAN DE GEGEVENS DOOR DE KANS KLEINER TE MAKEN DAT ER MEE GEROMMELD WORDT'

Papa's mail

Maar 'rommelen' is niet altijd bewust kwaadaardig: tegenwoordig mogen kinderen van sommige ouders wel 'even met de tablet van papa een spelletje doen'. Maar wat nu als dat kind ook papa's mail kan openen en bewerken? Of bedrijfsgegevens kan openen? De risico's van dat spelen kunnen groter zijn dan je zou denken. Want dat kind kan de tablet ook gebruiken om even zijn of haar social media pagina's te bekijken, en dan kan er van alles aan malware worden meegenomen. Daarom moet de IT-afdeling voorkomen dat malware die op een of andere manier op privé-apparatuur is geïnstalleerd, wordt overgebracht op zakelijke applicaties, gegevens of netwerken. Niet alleen bewust kwaadwillenden kunnen BYOD misbruiken om virussen en dergelijke in netwerken te brengen, dat kan ook onbewust gebeuren. Het resultaat is er niet minder dramatisch om.

Scan

Wanneer een privé-laptop of desktop wordt aangesloten op een virtual private network (VPN), moet deze eerst grondig gescand worden om te garanderen dat het operating system een ondersteunde versie is en dat alle updates zijn uitgevoerd. Die scan kan ook vaststellen of er een afdoende virusbescherming is en er een effectieve firewall is opgezet. Maar voer ook scans uit om zwakke plekken in die afscherming te vinden. Mobiele devices met potentieel schadelijke toepassingen moeten kunnen worden geblokkeerd; maak gebruik van zogenoemde 'application blacklisting' om het BYOD en BYOPC beleid te handhaven.

Zorg dat content die wordt geüpload vanaf privé-apparaten wordt gescand op malware. De kwaadwillende ontwikkelaars van schadelijke software zijn heel slim in het verbergen van hun programma's in schijnbaar bona fide software, zogenoemde trojans. Daarom moet een IT-afdeling ook gebruik maken van zogeheten 'behavior-based' detectie: kunnen zien hoe een programma zich gedraagt. Een schadelijk programma zal zich verraden door zijn afwijkende gedrag.

Betuttelend

Maar zoals met veel zaken is de mens de zwakste schakel in een keten. Nog veel te veel mensen zijn te gemakkelijk met privé-apparatuur die ze gebruiken voor hun werk. Daarom moet dat BYOD-beleid ook benadrukken dat de gebruiker een grote eigen verantwoordelijkheid heeft. De IT-afdeling kan niet alles constant controleren, al is het wel raadzaam om regelmatig die privé-apparaten in te nemen om ze te checken op malware. Dat klinkt betuttelend, maar zoals al eerder gemeld: die malware hoeft niet bewust te zijn gedownload. Iemand kan heel zorgvuldig met zijn devices omgaan, alles volgens de regels doen die de IT-afdeling heeft geformuleerd. Maar die kwaadwillenden zijn heel slim, kunnen hun malware in de meest schijnbaar onschuldige berichtjes verstoppen. Een melding die van een creditcard-bedrijf afkomstig is lijkt te zijn, of zelfs van de Belastingdienst of nog erger: het CJIB, kan grote schade aanrichten als dat geopend wordt. Daarom is voorlichting van de eigen IT-afdeling ook belangrijk. En als iemand vermoedt dat er op een of andere manier stiekem toch malware op zijn privé-apparaat is geïnstalleerd, moet hij niet bang zijn dat te melden aan de leidinggevende en de IT-afdeling. Bewust malware op het netwerk proberen te planten mag best hard worden aangepakt, desnoods met ontslag op staande voet, maar als de gebruiker zijn onschuld kan aantonen, moet er ook clementie kunnen worden getoond. Sterker nog: die persoon zou beloond moeten worden voor zijn eerlijkheid, en dat hij het bedrijf heeft behoed voor mogelijk ernstige schade. ■