ICT-SECURITY WHITEPAPER

BNS hybrIT
INFRA ● SOFTWARE ● CLOUD

Ja,
ook u bent een doelwit voor hackers!

19 tips om uw ICT-infrastructuur te beveiligen tegen hackers en ransomware

Microsoft Gold Partner | WatchGuard | Lepide | FocusCenter | audiocodes

Inhoud

Ja,

ook u bent een doelwit voor hackers!

Stop met uzelf af te vragen of uw bedrijf een doelwit kan zijn voor hackers. Het antwoord is volmondig, ja! Van het kleinste familiebedrijf tot de grootste multinational. Cybercriminelen versturen nog steeds massaal malafide e-mails de wereld rond die in ieders mailbox terecht kunnen komen. Dagelijks worden bedrijven in België gegijzeld met hun eigen data. De hackers vragen vaak duizenden euro's losgeld om deze bedrijfsgegevens terug te krijgen.

Natuurlijk blijft ICT-security een permanente afweging tussen flexibiliteit, gebruiksvriendelijkheid en veiligheid van uw netwerk en documenten. Een afdoend en up-to-date beveiligingsplan is met andere woorden een must. We kunnen u namelijk garanderen dat ook uw organisatie op de radar staat van deze hackers. Het is aan u om ze buiten te houden. Gelukkig zijn er de laatste jaren zeer veel nieuwe mogelijkheden bij gekomen om u te beveiligen, zonder dat dit afbreuk doet aan uw interne werking.

Start vandaag met de beveiliging van uw ICT-processen. In deze whitepaper geven we u alvast enkele tips om van start te gaan. En het hoeft zelfs niet veel geld te kosten...

Heeft u hulp nodig bij het uitvoeren van deze tips?
Dan helpen wij u graag verder.

Bel ons op +32 11 858 850.

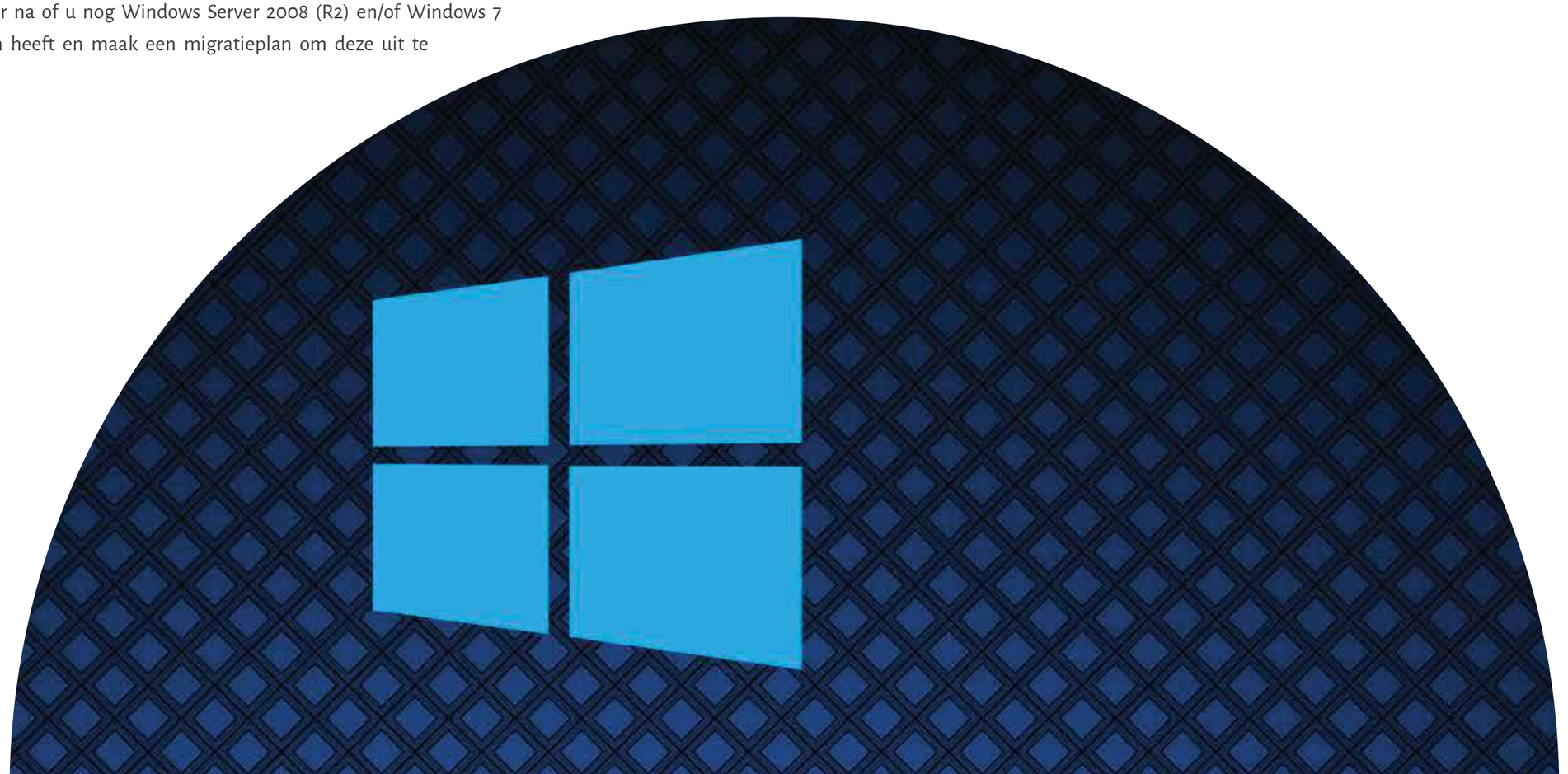
Tip #1

Upgrade Windows Server 2008 (R2) en Windows 7

Windows Server 2008 werd op 27 februari 2008 gelanceerd. Bijna 12 jaar na datum wordt op 14 januari 2020 de ondersteuning op Windows Server 2008(R2) en Windows 7 stopgezet. Dit lijkt misschien nog veraf, maar een server OS vervangen gaat niet zo snel. Met andere woorden, nu is het moment om hier mee aan de slag te gaan. Na 14 januari 2020 worden er geen beveiligingsupdates meer uitgerold voor deze besturingssystemen en zijn uw systemen niet langer optimaal beveiligd.

Hou er ook rekening mee dat zeer veel 3rd party software (antivirus, back-up, ERP, boekhouding, enz.) op 14 januari stopt met het supporteren van deze platformen. Hoe minder platformen ze moeten supporteren, hoe lager hun supportkost. Het is vaker dat er zich problemen voordoen met deze 3rd party software dan met het Windowssysteem zelf.

Kijk zeker na of u nog Windows Server 2008 (R2) en/of Windows 7 systemen heeft en maak een migratieplan om deze uit te faseren.



Tip #2

Beperk het aantal domain administrators

Er zouden geen dagelijkse gebruikersaccounts lid mogen zijn van de groep domain administrators. Leden van de groep domain administrators hebben lokale beheerdersrechten op elk gekoppeld systeem (werkstation, servers, laptops, enz.) en dit is een zeer groot risico op 'onvrijwillige' fouten. Een hacker die toegang krijgt tot een login die lid is van de groep domain administrators, kan aan al uw systemen! Vermijd dit te allen prijze.

Het proces om accounts uit de domain administrators groep te verwijderen is niet eenvoudig. Om dit proces te vergemakkelijken, hebben we enkele scripts ontwikkeld die u hierbij kunnen helpen. Ze zullen u een beter overzicht geven van alle domain administrators en waar deze gebruikt worden. Daarna kan u beginnen met het deactiveren van accounts. Liefst één voor één. Het kan een pijnlijk proces zijn, maar het is het zeker waard!

Tip #3

Patch en installeer tijdig (security) updates

Patch management is een belangrijk onderdeel in het beveiligen van systemen en netwerken. Het tijdig patchen en installeren van (security) updates is noodzakelijk om uw systemen en netwerken maximaal te beschermen. Het patch management systeem moet daarom zo efficiënt mogelijk zijn.

Patch management bestaat uit:

- Scannen van de situatie. Hoe sta ik ervoor?
- Beoordelen van de gevonden zwakheden (en geadviseerde patches).
- Toepassing van de noodzakelijke patches.
- Testen van systemen na installatie van patches. Ze kunnen de werking van applicaties beïnvloeden.
- Rapportage.

Dit proces dient periodiek herhaald te worden. De frequentie hiervan wordt bepaald door het securitybeleid dat een organisatie volgt.

Ondanks het feit dat patches uitgebreid gevalideerd worden, kunnen ze in uitzonderlijke gevallen (of specifieke omgevingen) leiden tot meer problemen dan dat ze oplossen. Dan moet u kunnen terugvallen naar een snapshot of goede back-up.

Het BNS **FocusCenterMonitoring (FCM)** systeem biedt ondersteuning in het patch management van onze klanten. Essec FCM deelt patches op in verschillende groepen, waarvan wij volgende patches installeren: **security updates**, **critical updates** en **service packs**.

> *FocusCenterMonitoring biedt ondersteuning bij het uitrollen van patches en updates*

FocusCenter
You are in control

FocusCenter beheert en bewaakt 24u op 24u de kritieke ICT-componenten van uw infrastructuur. Het is een geautomatiseerde applicatie voor ICT-systeembeheer die opgebouwd is rond twee pijlers:

1 - Het bewaken van de kritische ICT-systemen

Met een team van System Engineers bewaken en onderhouden we 24u op 24u de PC's, servers, routers, switches, firewalls en netwerken van onze klanten. Alle activiteiten zijn er op gericht om problemen te voorkomen of problemen op te lossen nog voor de bedrijfsvoering in gevaar komt. Deze proactieve benadering wordt optimaal ondersteund door FCM.

2 - Het inventariseren van uw ICT-infrastructuur (hard- en software)

Met FocusCenter is het ook mogelijk om u een gedetailleerde inventaris van uw hardware, software en licenties te geven.

Meer info over FocusCenter op onze website

Tip #4

Beveilig het domeinbeheerdersaccount

Elk domein bevat een beheerdersaccount. Dit account is standaard lid van de groep domain administrators. Het ingebouwde beheerdersaccount mag alleen worden gebruikt voor het instellen van domeinen en voor noodherstel (het herstellen van Active Directory).

Iedereen die op administratief niveau toegang tot servers of Active Directory nodig heeft, moet zijn eigen individuele account gebruiken.

Niemand mag het wachtwoord van de domeinbeheerder kennen. Stel een lang wachtwoord in van meer dan 20 karakters en berg het op in een kluis. Nogmaals, de enige keer dat u dit nodig heeft, is voor hersteldoeleinden.

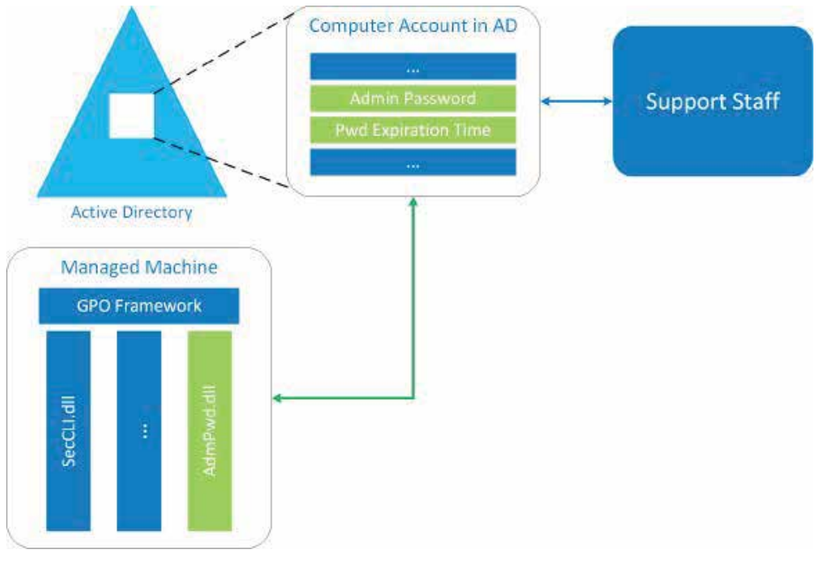
Tip #5

Gebruik Local Administrator Password Solution (LAPS)

Local Administrator Password Solution (LAPS) is een populaire tool voor het instellen van het lokale beheerderswachtwoord op alle computers.

Het komt vaak voor dat organisaties Windows installeren met behulp van images. Hierdoor kan snel een standaardconfiguratie op alle apparaten worden geïmplementeerd. Maar dit betekent vaak dat het lokale beheerdersaccount op elke computer hetzelfde is. Omdat het lokale Administrator-account de volledige rechten heeft tot een PC, is dit het enige wat een hacker nodig heeft om toegang te krijgen tot alle systemen.

LAPS is een Microsoft-tool die u assisteert in het beheer van de lokale accountwachtwoorden van computers die met het domein verbonden zijn. Het zal een uniek wachtwoord instellen voor elk lokaal admin account en die opslaan in Active Directory. LAPS is gebaseerd op de Active Directory. Het is dus niet nodig om extra servers te installeren.



Location Administrator Password Solution diagram

Tip #6

Maak gebruik van een standaard- en een beheerdersaccount

Als ICT-medewerker mag u niet elke dag inloggen met een lokale beheerdersaccount of met een account die over bevoorrechte toegang beschikt (domain administrator). Maak in plaats daarvan twee accounts aan. Een normale account zonder beheerdersrechten en een geprivilegieerd account dat alleen voor administratieve taken gebruikt wordt.

Maak gebruik van een **niet-beheerdersaccount** voor uw dagelijkse taken zoals het behandelen van e-mails, browsen op het internet, gebruik van ticketsystemen, enzovoort. Maak alleen gebruik van een geprivilegieerd beheersaccount wanneer u beheertaken moet uitvoeren zoals het aanmaken van een gebruiker in Active Directory, het inloggen op een server, het toevoegen van een DNS-record, enzovoort. Door simpelweg een regulier account te gebruiken, kunt u de veiligheid verhogen en voorkomen dat u ernstige fouten maakt.

Tip #7

Start met een Audit policy en bewaak Active Directory gebeurtenissen

Om abnormaal gedrag op uw netwerk vast te stellen, controleert u best op regelmatige basis volgende Active Directory gebeurtenissen:

- Wijzigingen in geprivilegieerde groepen zoals domain administrators, bedrijfsadministrators en schemabeheerders.
- Een piek in foutieve paswoorden.
- Een piek in locked-out accounts.
- Uitschakeling of verwijdering van antivirussoftware.
- Log on/Log off events.
- Gebruik van lokale beheerdersaccounts.

De beste manier om dit te beheren, is door het verzamelen van alle logboeken op een centrale server om vervolgens rapporten te genereren met behulp van een log-analysesoftware. **Lepide Auditor** is een van de tools die u inzicht verschaft in deze logbestanden.

Lepide

Lepide Auditor *biedt één gecentraliseerde console waarmee u uw Active Directory, Group Policies, Exchange, SharePoint, SQL Server en Windows File Server kan controleren. Het bevat ook tal van specifieke rapporten die u kunnen helpen bij het voldoen aan aspecten van GDPR-conformiteit.*

Het actuele machtigingsrapport bijvoorbeeld, toont alle huidige machtigingen van gebruikers op gedeelde bestanden, mappen in bestandsserver en mailboxen op Exchange Server. Naast de actuele, krijgt u ook een lange termijn overzicht van wijzigingen die zijn aangebracht in de configuratie van servercomponenten. Bijvoorbeeld toegang tot de gegevens en wijzigingen in toestemmingen van gebruikers/objecten. U kan ook realtime meldingen verzenden via e-mail indien er updates zijn voor bepaalde tabbladen of apps.

Wilt u meer weten over Lepide Auditor of wenst u graag een live demo?
Geef ons een seintje op +32 11 858 858

Tip #8

Gebruik Multi Factor Authentication voor Remote Access

Acht tekens met complexiteit is niet langer een veilig wachtwoord. Hoe langer het wachtwoord, hoe beter, maar niemand kan ze nog onthouden. Het toevoegen van een Multi Factor Authentication (MFA) is dan ook steeds vaker aan te bevelen. Zeker voor Remote Access.

Bij veel clouddiensten is MFA standaard inbegrepen (ook bij Office 365 kan dit gratis geactiveerd worden) en voor een kleine meerprijs kan u MFA ook toevoegen aan uw 'on-prem' servers.

> *Acht tekens met complexiteit is niet langer een veilig wachtwoord.*

Tip #9

Blokkeer Remote Access voor domain administrators

Leden uit de groep domain administrators mogen extern geen toegang krijgen. Niet via RDS, Citrix, VPN of andere technologieën. Als zo'n account in verkeerde handen terecht komt, dan is het installeren van een cryptovirus een fluitje van een cent.

Remote Access is voorbehouden aan user accounts, liefst met een MFA-oplossing. Na een correcte login, kunnen er serviceactiviteiten gebeuren met een administrator account.

Tip #10

Schoon oude Active Directory gebruikers op

U moet een procedure hebben om ongebruikte gebruikers- en computeraccounts in Active Directory te detecteren. Laat geen ongebruikte accounts in Active Directory zitten tot een hacker ze kan misbruiken om uw systemen te ontwrichten. Gebruik Azure AD connect voor een Single Sign-On ervaring met meer dan 200 Cloud providers.

> *Laat geen ongebruikte accounts in Active Directory zitten*

Tip #11

Gebruik Office 365 Secure Score

Office 365 Secure Score analyseert uw Office 365-services, controleert vervolgens uw instellingen en activiteiten en geeft u een beveiligingsscore op basis van activiteiten- en beveiligingsinstellingen. Daarnaast krijgt u een gedetailleerde lijst met aanbevolen acties om de beveiliging te verbeteren.

U hebt een Premium- of Enterprise-abonnement nodig om toegang te krijgen tot deze functie. Bovendien moet u de globale beheerder zijn of aangepaste rol toegewezen krijgen. Als u toegang hebt tot deze functie, profiteer er dan van. Niet tevreden van uw score? Contacteer ons.

Tip #12

Gebruik de nieuwste ADFS- en Azure beveiligingsfuncties

ADFS en Azure hebben enkele geweldige beveiligingsfuncties. Natuurlijk hebben de premiumabonnementen de meest uitgebreide mogelijkheden. Het maakt echter niet uit welke versie van Office 365 u heeft. Er zijn steeds functies die de moeite waard zijn om te bekijken:

- **Smart Lockout** gebruikt algoritmen om ongebruikelijke aanmeldingsactiviteiten te herkennen.
- **IP Lockout** gebruikt de database van bekende kwaadaardige IP-adressen van Microsoft om logins te blokkeren.
- **Aanvalsimulaties**: U kan phishingtests uitvoeren om eindgebruikers te trainen. (ATP Plan 2)
- **MFA-verificatie**: De Two-Factor Authenticatie oplossing van Microsoft.
- **Verboden wachtwoorden**: Controleert wachtwoorden op een bekende lijst.
- **Azure AD Connect Health**: biedt verschillende goede rapporten.

Bekijk zeker alle beschikbare beveiligingsfuncties in ADFS, Office 365 en Azure. Een prima toevoeging aan alle abonnementen is ATP Plan 1 voor € 1,69 per gebruiker per maand*. Ook 'Safe attachments' en 'Safe links' zijn uitstekende toevoegingen aan uw e-mailbeveiliging.

*prijs op datum van druk (08/2019)

Wilt u meer weten over het ATP-programma van Microsoft? Bekijk dan deze uitgebreide video waarin Jeremy Chapman haarfijn uitlegt hoe ATP kan bijdragen tot de beveiliging van uw organisatie.

Scan de QR-code om de video te starten.

Tip #13

Beveilig uw Cloudservices

Met onze Managed Hostings nemen wij de beveiliging van uw Cloudservices voor u in handen. Op afgesproken tijdstippen zorgen we voor de nodige beveiligingsupdates en wordt de correcte werking van de website door een professional opgevolgd en gerapporteerd. Bovendien staan deze hostings in een volledig gescheiden omgeving, in een iso27001 gecertifieerd datacenter.

Tip #14

Gebruik Microsoft Bitlocker

Indien uw niet-versleutelde laptop wordt gestolen of indien u deze verliest en u niet kan uitsluiten of er persoonsgegevens op staan, dan moet u dit volgens de nieuwe GDPR-wetgeving onherroepelijk melden aan de bevoegde instanties.

Microsoft Bitlocker is een standaardoplossing die u al in uw bezit heeft. Het maakt gebruik van de TPM-technologie (Trusted Platform Module), die gebaseerd is op de beveiliging van hardware door middel van cryptografische sleutels. Deze cryptoprocessorchip bevat meerdere fysieke beveiligingsmechanismen om sabotage tegen te gaan.

De beste oplossing is om de encryptie centraal te beheren via een Active Directory Group Policy. Zo bepaalt u centraal de encryptiesleutel en kan u bij een hardware falen nog altijd de encryptie ongedaan maken en de data uitlezen. Als u de encryptiesleutel door de gebruiker zelf laat bepalen, zal u zien dat u de sleutel niet heeft als het nodig is.

Tip #15

Controleer uw firewall

Samen met een gespecialiseerd en onafhankelijk bedrijf kunnen we de beveiliging van de publiek toegang van uw netwerk controleren door een **PEN-test** uit te voeren. De testen gebeuren volgens officiële en erkende standaarden zoals OWASP OTG (Web Application Security Testing Guide) en PTES (Penetration Testing Execution Standard).

De consultants beschikken over de volgende certificaten:

- OSCP (Offensive Security Certified Professional),
- GXPN (Exploit Researcher and advanced penetration tester),
- ECSA (Certified Security Analyst),
- CEH (Certified Ethical Hacker) certified.

De doelstelling van de test is om de beveiligingsstatus van uw publiek toegankelijke infrastructuur te controleren:

- Welke gegevens en systemen worden blootgesteld aan echte aanvallers?
- Door middel van actieve en passieve verkenning zullen we uw blootgestelde infrastructuur identificeren en evalueren voor misconfiguraties in de beveiliging, alsook voor andere kwetsbaarheden.

Tijdens de PEN-test wordt gebruik gemaakt van volgende testmethodiek:

- Verkenning en nazicht via publieke bronnen (OSINT - open source intelligence).
- Identificeren van kwetsbaarheden.
- Analyse & validatie van de kwetsbaarheden.
- Uitbuiting en data exfiltration.

Een PEN-test controleert de beveiliging van uw publiek ICT-infrastructuur

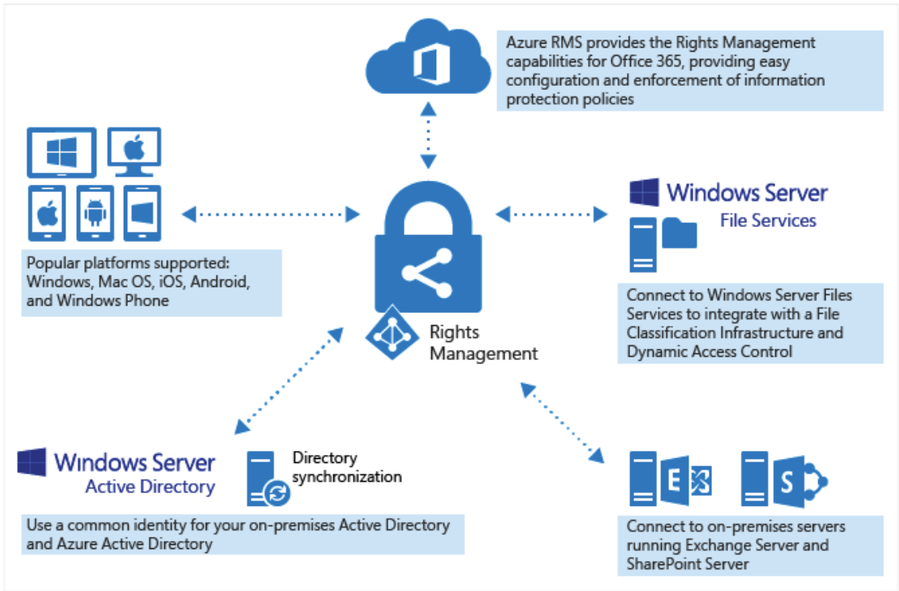
Tip #16

Beveilig het document, niet de locatie

Het beveiligen van 'reizende' data (Cloud, USB-sticks, e-mail, e.d.) is al langer een probleem en ook hier kan encryptie toegepast worden. Niet enkel in het kader van GDPR, maar zeker ook in het kader van de bescherming van uw eigen intellectuele eigendom.

Wie kent niet de verhalen van de accountmanager die nog in het bezit is van klantenlijsten van zijn vorige werkgever of prijslijsten die bij de concurrentie terecht komen. Allemaal scenario's die iedere werkgever wil vermijden.

Uiteindelijk willen we documenten niet beveiligen op basis van de plaats waar ze staan (zoals nu in een fileserver of op SharePoint), maar wel het document zelf. Met RMS kan dit volledig geautomatiseerd worden. Een prijslijst krijgt de rechten 'prijslijsten' en eender waar deze file terecht komt, blijven deze rechten behouden (op een USB-stick, in een mail, op een OneDrive, enz.). Zolang u tot de Active Directory securitygroep 'sales' behoort, heeft u hier toegang toe. Behoort u niet meer tot deze AD-groep, dan kan u het document niet meer openen.



Schematische voorstelling van Azure Rights Management protection

Tip #17

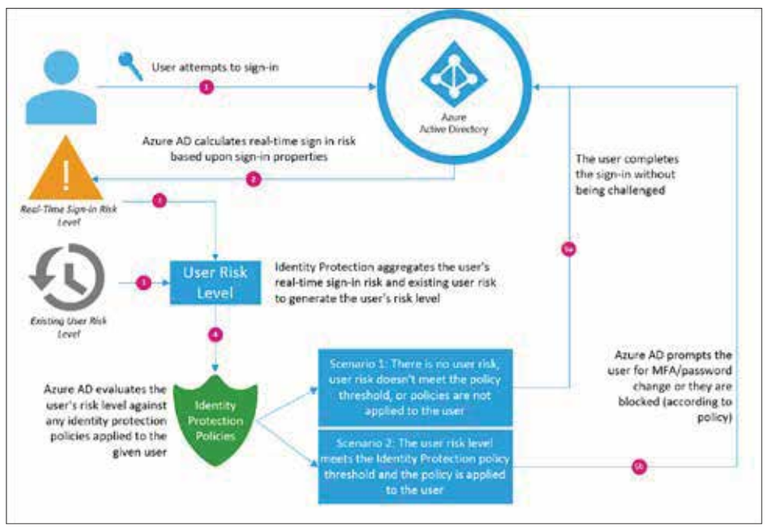
Activeer Azure Active Directory Identity Protection

De overgrote meerderheid van de security breaches vindt plaats wanneer hackers toegang krijgen tot een bedrijfsomgeving door de identiteit van een gebruiker te stelen. Door de jaren heen zijn hackers steeds efficiënter geworden in het gebruik van geavanceerde phishingfraude. Zodra een aanvaller toegang heeft tot gebruikersaccounts met 'slechts' lage toegangsrechten, is het relatief eenvoudig om toegang te krijgen tot belangrijke bedrijfsgegevens.

Wat moet u doen om dit te vermijden:

- Alle identiteiten beschermen, ongeacht hun toegangsrechten.
- Proactief voorkomen dat aangetaste identiteiten worden misbruikt.

Het ontdekken van gecompromitteerde identiteiten is geen gemakkelijke taak. Azure Active Directory maakt gebruik van adaptive machine learning algoritmen en heuristieken om anomalieën en verdachte incidenten te detecteren die wijzen op potentieel aangetaste identiteiten. Met behulp van deze gegevens genereert Identity Protection rapporten en waarschuwingen waarmee u de gedetecteerde problemen kan evalueren en de juiste maatregelen voor beperking of herstel kan nemen.



Schematische voorstelling van Azure Active Directory Identity Protection

Tip #18

Update uw communicatieserver (PBX/telefooncentrale)

Het is te allen tijde noodzakelijk om de software van uw communicatieserver up-to-date te houden. Installeer steeds de laatste security patches en voorkom zo onderstaande issues:

- Afluisterpraktijken
- Wijziging van Voice Stream
- Toll Fraude
- Omleiding van gesprekken
- Accounting data manipulatie
- Caller ID-verpersoonlijking
- Ongewenste oproepen en boodschappen
- Denial-of-Service (DoS) aanvallen

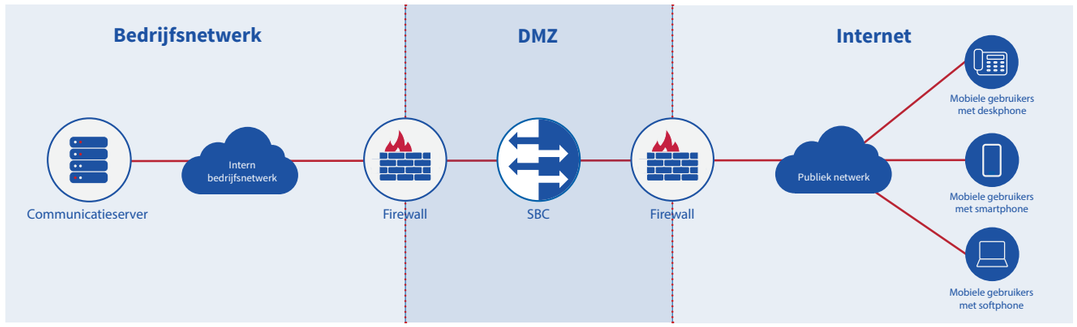
Tip #19

Beveilig uw communicatieserver met een SBC

Vroeger was de beveiliging van uw communicatienetwerk een eenvoudige klus. Maar met de komst van smartphones, tablets, VoIP en Cloud is deze beveiliging wat complexer geworden. Zeker in tijden van ransomware en hacking is een degelijke beveiliging van uw communicatiekanalen (VoIP/SIP/ISDN) geen overbodige luxe.

Een Session Border Controller kan hier een oplossing voor bieden. Een SBC kan u bekijken als de buitenwipper van uw netwerk. Het zorgt onder andere voor een fysieke scheiding tussen verschillende netwerken en beschermt uw bedrijfsnetwerk tegen aanvallen van buitenaf.
Daarnaast controleert een SBC de identiteit van inkomende en uitgaande gesprekken en handhaaft het uw beveiligingsbeleid aan de hand van black- & whitelists.

Het is ook mogelijk om een SIP-trunk te koppelen op een SBC waardoor u uw bestaande (IP)PBX kan blijven gebruiken, net als uw analoge telefoontoestellen. Tegelijkertijd kan er ook een nieuwe UC-omgeving worden opgezet die naadloos aansluit op uw analoge omgeving.



Schematische voorstelling van een communicatienetwerk met SBC

Ook dit nog...

Vergeet niet uw basisinfrastructuur te beveiligen

- Maak gebruik van een beveiligde **internetlijn**
- Zorg voor een goede **firewall**
- Gebruik performante **switches**
- Werk altijd met gepatchte **servers**
- Gebruik snelle **storage**
- Maak gebruik van veilige **cloudservices**

- Zorg voor een adequaat **backup beheer**
- Schaf een degelijke **antivirus** aan
- Denk na over uw **gebruikersbeheer**
- Hanteer de juiste **in- en uitdienstprocedure**
- Backup en beheer uw **PC's, tablets en mobiele toestellen** als een goede huisvader

BNS hybrIT

INFRA • SOFTWARE • CLOUD

www.mybns.com | sales@mybns.com | +32 11 858 850
Bisschopsweyerstraat 37, 3570 Alken

V.10.21