Exchange beveiliging; tips die je morgen direct kunt gebruiken!

Dave Stork

Experts Live 2016

Dave Stork

- Architect bij OGD ICT Diensten
- MVP en MCT
- Co-auteur Practical PowerShell Exchange 2016
- dave.stork@ogd.nl
- @dmstork
- Dirteam.com/dave

Inhoud

- Client – Server verbindingen
- Mailflow
- Server security
- Data security

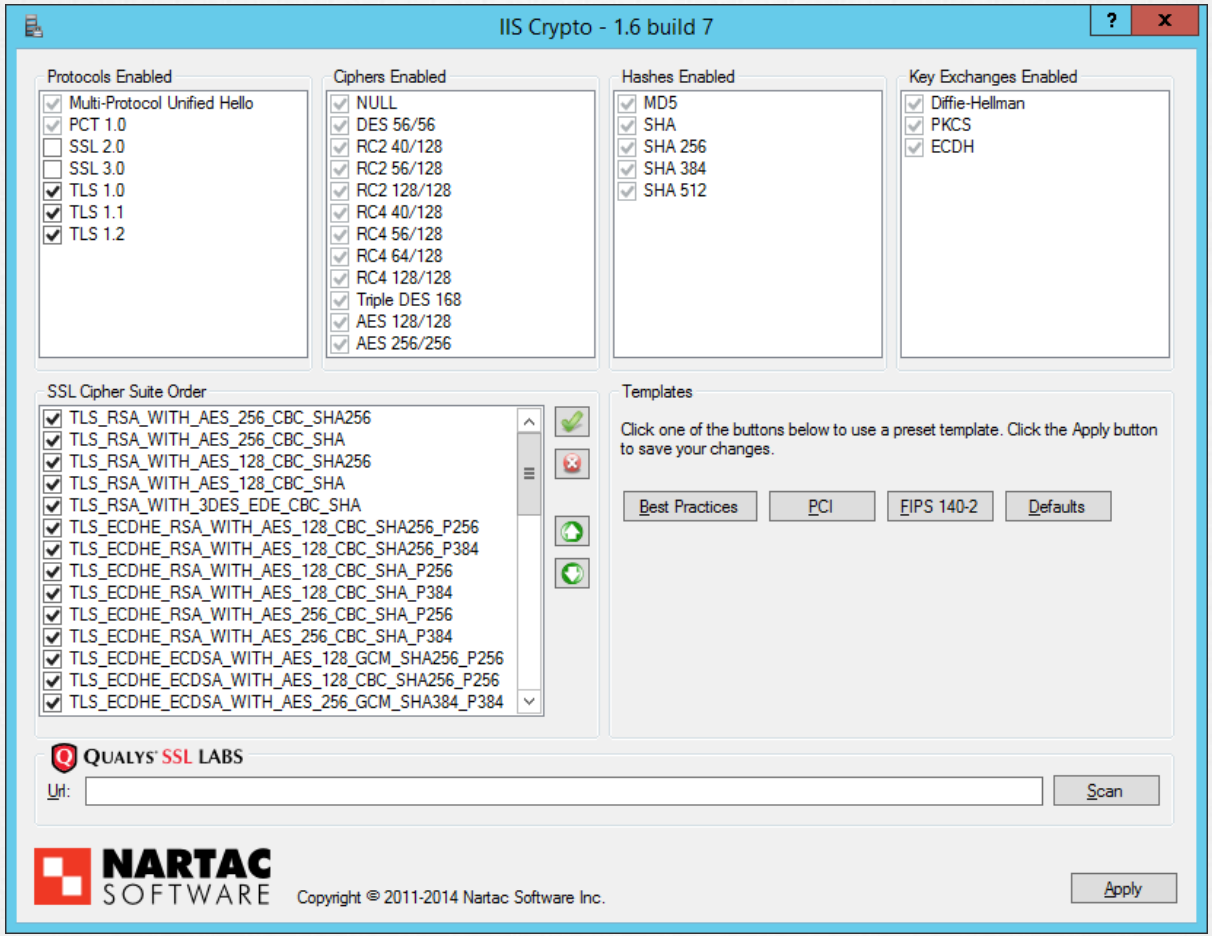
OFFICE 365

Client – Server verbindingen

Alle verbindingen zijn standard encrypted, maar…

- Let op verloop SHA1 certificaten per 2017
  - Vraag nieuwe certificaten aan met Exchange Tools
- Schakel SSL3, RC4 etc. op de server uit & optimaliseer cipher order.
  - Let op: schakel TLS1.0 niet uit op Exchange servers!
- Zijn er voor intern en extern verschillende eisen qua encryptie, gebruik dan de reverse proxy/load balancer hiervoor.
- Controleer deze settings weer na updaten Exchange.

- HTTPS
  - Webmail (OWA)
  - Outlook Anywhere / MAPI over HTTP
  - ActiveSync
- Wees bekend met welke clients/Exchange protocollen nodig zijn en maak keuze of ze extern noodzakelijk zijn.
- IMAP/POP Keuze tussen implicit en explicit TLS
  - Implicit = Secure IMAP; TCP 995
  - Explicit = IMAP over TLS; TCP 143
- SMTP Client submission via TCP 587


IIS Crypto - 1.6 build 7
Protocols Enabled
Multi-Protocol Unified Hello
PCT 1.0
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
Ciphers Enabled
NULL
DES 56/56
RC2 40/128
RC2 56/128
RC2 128/128
RC4 40/128
RC4 56/128
RC4 64/128
RC4 128/128
Triple DES 168
AES 128/128
AES 256/256
Hashes Enabled
MD5
SHA
SHA 256
SHA 384
SHA 512
Key Exchanges Enabled
Diffie-Hellman
PKCS
ECDH
SSL Cipher Suite Order
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
Templates
Click one of the buttons below to use a preset template. Click the Apply button to save your changes.
Best Practices
PCI
FIPS 140-2
Defaults
QUALYS SSL LABS
Url:
Scan
NARTAC SOFTWARE
Copyright © 2011-2014 Nartac Software Inc.
Apply

OFFICE 365

Administrator: Command Prompt - openssl s_client -connect webmail.lab2010.com:143 -starttls imap

```
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
CONNECTED(00000138)
depth=0 C = NL, ST = NH, L = Amsterdam, O = Lab2010, OU = IT, CN = webmail.lab20
10.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = NL, ST = NH, L = Amsterdam, O = Lab2010, OU = IT, CN = webmail.lab20
10.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/C=NL/ST=NH/L=Amsterdam/O=Lab2010/OU=IT/CN=webmail.lab2010.com
   i:/DC=com/DC=lab2010/CN=rootca
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFeTCCBGGgAwIBAgIKYQRm1AAAAAAABTANBgkqhkiG9w0BAQsFADA/MRMwEQYK
CZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHbGFiMjAxMDEPMA0GA1UE
AxMGcm9vdGNhMB4XDTE1MDQxOTE5MjQzOFoXDTE3MDQxODE5MjQzOFowazELMAkG
A1UEBhMCTkwxCzAJBgNVBAgTAk5IMRIwEAYDVQQHEwlBbXN0ZXJkYW0xEDAOBgNV
BAoTB0xhYjIwMTAxCzAJBgNVBAsTAklUMRwwGgYDVQQDExN3ZWJtYWlsLmxhYjIw
MTAuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvjozOMsLMeQ1
ObH7UfYlqSy/fDM++aABG1BVmFCVzcSa+f8+LrBehDOxYci8+uvq/oidX4GLHG6i
8Cltc1xxdyMHpESmBlnoZtNSl3Tba9RVOIbLw2YSqKxEeDxXjMvdsKgQieGdBF5U
CYtx5/8/zuB0wszo2syrw9UAPnkZ9PG5ZLt7t9g5/1m/bgMUFFp2cEbWb6kAsJuO
xrRuVnItl21XljplZlQkf8hZFbCeHbAdNBPXGSHTkEKnnl0FKQmUhI2+f1MyInSt
iyd9WF+Uq/dEkDA72M+fR+j6HJ7FHR4mqjtFeSfSILUfi38q/UjBQn0o5m+htpp1
ZY4+i9nvrwIDAQABo4ICSTCCAkUwDgYDVR0PAQH/BAQDAgWgMB0GA1UdDgQWBBQo
OE3pR/WbPr6NDwERL2c0/iSCkTA4BgNVHREEMTAvghN3ZWJtYWlsLmxhYjIwMTAu
Y29tghhhdXRvZGlzY292ZXIubGFiMjAxMC5jb20wHwYDVR0jBBgwFoAUA1y05Cdf
GhLmqeaZUhLe6YHxU2YwgcUGA1UdHwSBvTCBujCBt6CBtKCBsYaBrmxkYXA6Ly8v
Q049cm9vdGNhLENOPUwxMC1EQzAxLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBT
ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYjIwMTAs
REM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz
cz1jUkxEaXN0cmlidXRpb25Qb2ludDCBuAYIKwYBBQUHAQEEgaswgagwgaUGCCsG
AQUFBzAChoGYbGRhcDovLy9DTj1yb290Y2EsQ049QUlBLENOPVB1YmxpYyUyMEtl
eSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9bGFi
MjAxMCxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRp
ZmljYXRpb25BdXRob3JpdHkwIQYJKwYBBAGCNxQCBBQeEgBXAGUAYgBTAGUAcgB2
AGUAcjATBgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQsFAAOCAQEAnhcp
JlNeTvVnug9Kxgmj24fdrJfj0p2xSSELDVWwDYA1V+rJRnDvZM2bpC4IP0RX7qqG
2U5k4T+Hzz3HiRyxE/F0r2IWxqZPpdTtfU6iYfMYwIvJA7C307oEz4QlYrJ0HuEW
H4ygSLTDV7tW5mAx/DOTKV8io7RwYJ4owVnzSeQG8U16ciB1vGmVxrY8ETiVxyCu
1/Mdp4JVy7P5Ml6sPEmzGzjp8DiAfvhdt2w9eO/V+C8iT/6CHpTk4DxTBG18Qj2n
6YWDV57XL6Y5WFBAit7xBlrdtc7+We9fGPwvl0CZZc1qzYdkkGQSCkC5ML4a5CPl
bpHkvsHwmlQmvFamFw==
-----END CERTIFICATE-----
subject=/C=NL/ST=NH/L=Amsterdam/O=Lab2010/OU=IT/CN=webmail.lab2010.com
issuer=/DC=com/DC=lab2010/CN=rootca
---
No client certificate CA names sent
---
SSL handshake has read 1772 bytes and written 699 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA

Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES256-SHA
    Session-ID: C34700000785BFDEEAB2FA6C19D52040A5E5DA4AFD664239640F684A8DE9EA81A

    Session-ID-ctx:
    Master-Key: A23E74182962A9AEB9DFD91BF89F1A76DF98593C63DD9E1B4A26E1CDB3BF0ACC
9B7ACAFA7CEC755EAE9CE9D20D3A81DA
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1433697636
    Timeout   : 300 (sec)
    Verify return code: 21 (unable to verify the first certificate)
---
. OK CAPABILITY completed.
* BYE Connection is closed. 13
read:errno=0

C:\OpenSSL-Win32\bin>
```

Proxy, Load Balancer, Application firewall

- Security
- Pre-authentication
- Load balancing (availability)
- SSL Bridging
  - SSL endpoint in “appliance”, opbouw SSL sessie naar Exchange
  - maakt content filtering/switching mogelijk
- SSL Offloading
  - SSL endpoint in “appliance”, *geen* SSL sessie naar Exchange

MFA on-premises?

- Multi-factor authentication: token/apps/sms etc..
- Alleen voor webmail: /OWA en /ECP
- Let erop dat andere Exchange protocollen gebruikt door Outlook en ActiveSync niet beschermd worden.
  - Bijv. /EWS o.a. gebruikt door Outlook for Mac, of AutoDiscover.

- Toekomst? Waarschijnlijk Modern Authentication zoals in Office 365 gebruikt word. Helaas nu nog niet ondersteund.
  - VPN oplossingen

Certificate Based Authentication

ActiveSync

- In plaats van username/wachtwoord een certificaat ter authenticatie.
- Is dus GEEN MFA
- Wachtwoord change geen impact
- Wel een PKI infrastructuur nodig
- User Certificaat moet gemaakt en uitgedeeld worden op device

OFFICE 365

Mailflow

Opportunistic TLS SMTP

- EHLO response FQDN
- Certificaat met domeinnaam gelijk aan EHLO
- Hoeft geen trusted certificaat te zijn
- Altijd fallback naar unencrypted SMTP

Mutual TLS / Domain Security

- Per mail domein
- Per ontvangende partij
- Uitwisseling public keys
- Send & Receive connector

SPF

- Sender Policy Framework
- Anti-spoofing
- TXT record in mail domein
- Definieert servers die mogen mailen namens domein
- Op basis van From:

DKIM

- Domain Keys Identified Mail
- Signeert uitgaande mail
- Controleert inkomende mail
- Public key in DNS

- Hogere zekerheid dat afzender niet gespooft is
- Controle of bericht is aangepast na signeren

DMARC

- Domain-based Message Authentication Reporting and Conformance
- Leunt op SPF en/of DKIM
- Rapportages van ontvangers wanneer mail DMARC heeft gefaald

S/MIME

- User level signeren en encryptie van mails
- Certificaat gebaseerd
- Zender en ontvangen moeten elkaars certificaat hebben (public key) worden voor encryptie mogelijk is
- Veel oplossingen voegen wijzigingen toe aan mail, waardoor signeren faalt
- Omslachtig

Office 365 Message Encryption

Of third party tools

- Mail via appliance
- Die stuurt link door naar geaddresseerde
- Geaddresseerde logt in op appliance en leest mail etc.
- Antwoorden via appliance.

Malware etc. filtering

- Cloud service of appliance
- Op Exchange zelf
- Exchange Online Protection (EOP)
  - Met Advanced Threat Protection (ATP)
  - vervanging van links naar safelinks
  - Detonation van attachments

OFFICE 365

Server security

Redundantie

- Database Availability Group
  - Meerdere kopieen van databases mogelijk
  - Stretched in ander datacenter
- Back-up
  - Exchange Native Data Protection:
    - 2 kopieën in Datacenter 1
    - 1 kopie in datacenter 2
    - 1 vertraagde kopie (lagged copy) in datacenter 2
  - Exchange heeft dan zelf off-site point in time back-up

Back-up

- Dynamic data via VSS writers (Exchange aware)
  - Databases
  - Log files
  - Config files
- Snapshots van VMs niet te gebruiken
- Disaster recovery install

Anti-virus

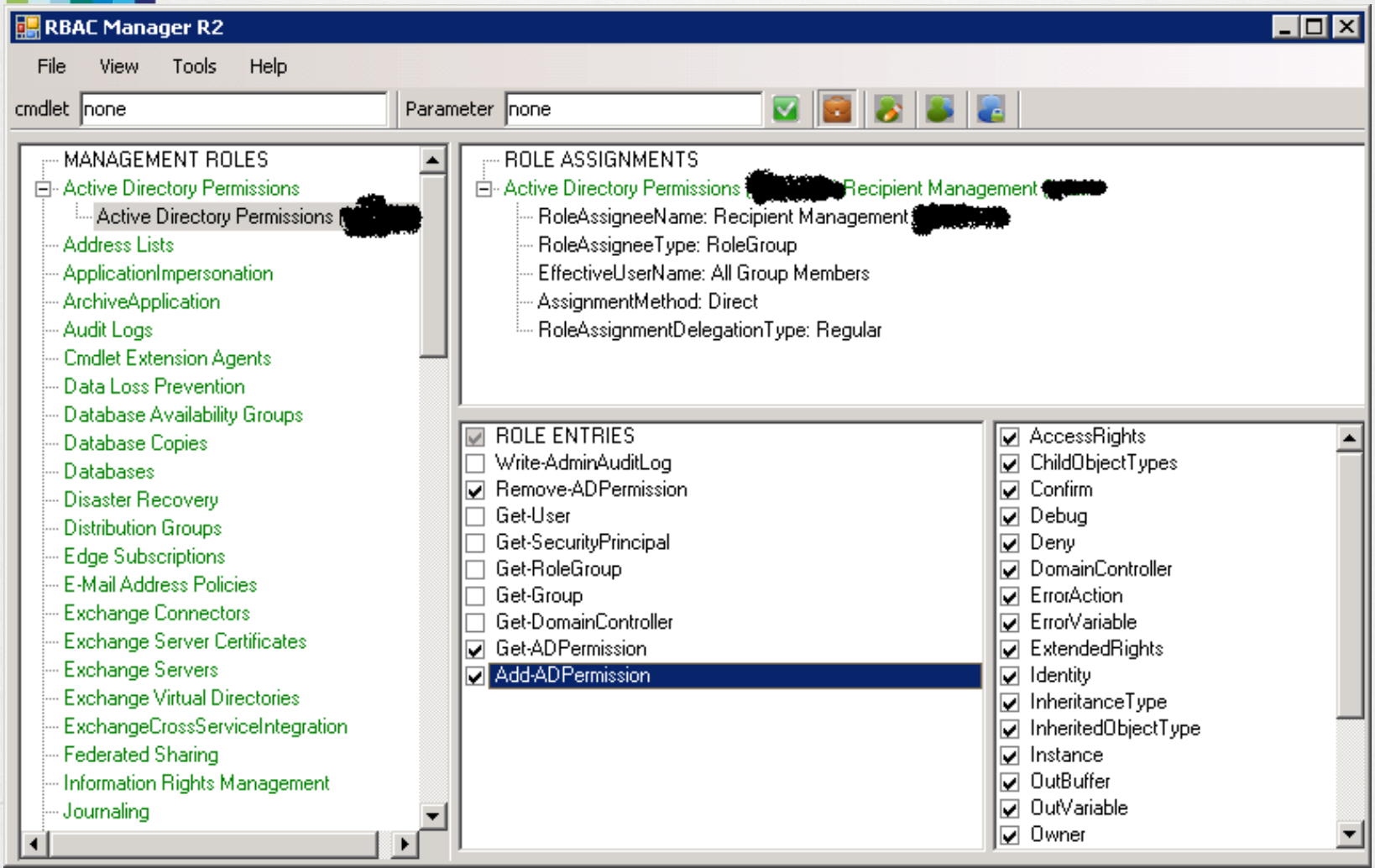
- On-access
- Cruciaal: Exchange exclusions
  - Paden
  - Bestanden en extensies
  - Processen
    - Vergeet back-up agent niet
- Exchange aware
  - SMTP scanning
  - Database scanning

Bitlocker

- Is ondersteund vanaf Exchange 2013
- Data at rest
- Let wel: mogelijke issues bij bepaalde HA features (AutoReseed)

Role Based Access Control

- Rechten op basis van rollen en groepen
- Standaard rollen
- Configureerbaar
- Zeer granulair
  - Per PowerShell cmdlet én parameter
  - Per OU etc.

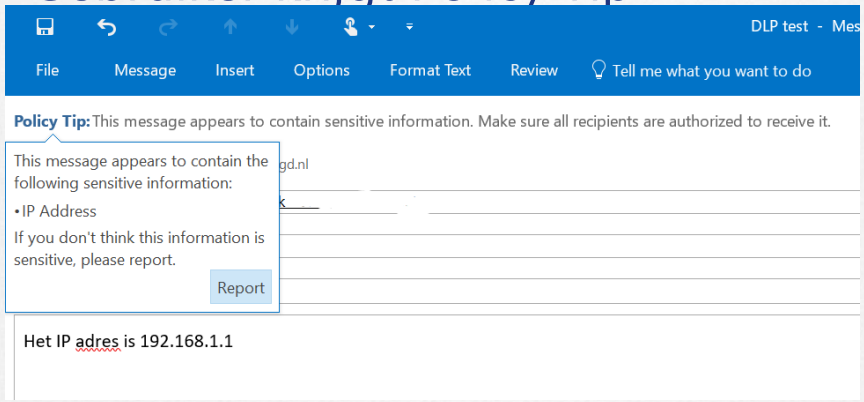

RBAC Manager R2
File
View
Tools
Help
cmdlet
none
Parameter
none
MANAGEMENT ROLES
Active Directory Permissions
Active Directory Permissions
Address Lists
ApplicationImpersonation
ArchiveApplication
Audit Logs
Cmdlet Extension Agents
Data Loss Prevention
Database Availability Groups
Database Copies
Databases
Disaster Recovery
Distribution Groups
Edge Subscriptions
E-Mail Address Policies
Exchange Connectors
Exchange Server Certificates
Exchange Servers
Exchange Virtual Directories
ExchangeCrossServiceIntegration
Federated Sharing
Information Rights Management
Journaling
ROLE ASSIGNMENTS
Active Directory Permissions
Recipient Management
RoleAssigneeName: Recipient Management
RoleAssigneeType: RoleGroup
EffectiveUserName: All Group Members
AssignmentMethod: Direct
RoleAssignmentDelegationType: Regular
ROLE ENTRIES
Write-AdminAuditLog
Remove-ADPermission
Get-User
Get-SecurityPrincipal
Get-RoleGroup
Get-Group
Get-DomainController
Get-ADPermission
Add-ADPermission
AccessRights
ChildObjectTypes
Confirm
Debug
Deny
DomainController
ErrorAction
ErrorVariable
ExtendedRights
Identity
InheritanceType
InheritedObjectType
Instance
OutBuffer
OutVariable
Owner

OFFICE 365

Data Security

Data Loss Prevention

- Voorkomen van per ongeluk mailen van vertrouwelijke informatie
- Op basis van functies en regex determineren of bijvoorbeeld credit card nummers vermeld zijn
- Gebruiker krijgt Policy Tip



Information Rights Management

- Per data object bepalen wat er mee mogelijk is
- Forwarding, printing etc.
- Wel een RMS infrastuctuur nodig.
- Voor externe gebruikers moet deze van buitenaf bereikbaar zijn
- Mocht men migreren van on-premises naar O365;
  - Hou on-premises intact
  - Stamp nieuwe objecten met O365 templates

Auditing

- Loggen welke handeling door wie is uitgevoerd
- Standaard actief op admin handelingen
- Te activeren op iedere mailbox
- Advies: altijd op Shared Mailboxen

Device Management

- Conditional Access
  - Compliant?
- Data control
  - Application Management
- Data Wipe
  - Full
  - Selective

Volgende sessie 11:30 – 12:30

Beheer Office365 snel, pijnloos en veilig met PowerShell

Maarten Visser

Experts Live 2016

Vragen?