IBM i Security

Common Nederland april 24 2017

common
NETHERLANDS

IBM i Security

- Reglementen
- Outsourcing
- Security Anno 1990’s
- Security Anno 2017
- Remediation

Reglementen and Compliance

- Handelt u uit veiligheidsoverwegingen of handelt u omdat u aan de reglementen wilt voldoen?
- GDPR
  - WBP
  - Datalek meldplicht
  - AVG
  - Boetes?
- GDPR – Persoonlijke data
- Financiële data
- Vertrouwelijke informatie
- Data integrity

common NETHERLANDS

Outsourcing

- Risco’s
- Verantwoordelijkheden

common
NETHERLANDS

IBM i is een veilig systeem!

- Maar eerst moet je het configureren!
- In 1990 was alles relatief makkelijk
  - Wired connections Twinax, Token Ring
  - Modem – Vaste lijn/kieslijn
  - Application driven security
  - Gebruikers access rechten
  - “Limited capabilities”
  - Secure WANs

IBM i is een veilig systeem!

- In 2017
  - Het Internet!
  - Hackers!
  - “Social Engineering”
  - Malware
  - TCP access
    - ODBC
    - SQL
    - SSH
    - FTP
    - WIFI
    - enz
  - Legacy systemen die nog draaien op security instellingen vanuit de jaren 90.

IBM i is een veilig systeem!

- Onvoldoende resources
- Weinig kennis
- Geen overzicht
  - van gegevensgevoeligheid
  - van kwetsbaarheid
- End of life!
- Andere prioriteiten
- Het zal ons toch nooit gebeuren!

IBM i Hacked! maart 2016

24 Maart 2016 werd de ‘security analysis’ team van Verizon gevraagd om de inbraak van de IBM i bij een grote waterzuiveringsinstallatie. Waar hackers toegang hadden geforceerd tot de gegevens van 300.000 klanten en toegang kregen tot de waterzuiveringssystemen waar ze controle namen over het volume van toegevoegde chemicaliën in het waterreservoir!

De IBM i is bestempeld als het veiligste systeem ooit gebouwd…

De beheerders van het IBM i systeem waren schuldig het systeem onvoldoende te hebben geconfigureerd of geen veilige omgeving hebben ingericht.

common NETHERLANDS

Wat kan ik doen??

- Een Risk Assessment
  - Analyseer alle onderdelen van het security systeem
  - Prioriteer gevoelige gegevens
  - Machtige gebruikersprofielen
  - Ongebruikte gebruikersprofielen
  - Network access points
  - Object rechten
  - “Adopted Authority”
  - Toegang tot het IFS

Wat vinden we

- Systeemwaardes te zwak
- Machtige gebruikersprofielen!
- Machtige gebruikersgroepen
- Gebruikersprofielen die jaren ongebruikt zijn (met wachtwoorden die onveranderd zijn!)
- Objecten (inclusief data bestanden) met *PUBLIC *ALL rechten
- Open toegang tot de IFS
- Actieve, onbeveiligde TCP servers
- Onvoldoende of geen auditing
- Audit entries niet bekeken

System Values

System Value	Current Value	Recommended Setting	Deviation from Recommendation (X)
QSECURITY	30	40 or 50	X
QALWOBJRST	*ALL	*ALWPTF or *NONE	X
QALWUSRDMN	*ALL	*ALL	
QAUTOCFG	0	0	
QAUTOVRT	20	0 or a fixed number	
QCRTAUT	*CHANGE	*USE or *EXCLUDE	X
QDSPSGNINF	0	0 or 1	
QFRCCVNRST	1	3	X
QINACTITV	30	30	
QINACTMSGQ	PSN001MQ F400	*DSCJOB	X
QDSCJOBITV	*NONE	60	X
QLMTDEVSSN	0	1	X
QLMTSECOFR	0	1	X
QMAXSIGN	3	5	
QMAXSGNACN	3	2 or 3	
QRETSVRSEC	1	0 or 1	
QRMTIPL	1	0	X
QRMTSIGN	*FRCSIGNON	*REJECT or *FRCSIGNON	
QRMTSRVATR	0	0	
QSHRMEMCTL	1	0 or 1	
QUSEADPAUT	*NONE	Authorization list name	X
QVFYOBJRST	3	3 or 5	

Machtige gebruikersprofielen

- PRTUSRPRF command gebruiken om QPSECUSR spoolfile te bekijken

```
                              Display Spooled File
File  . . . . . :   QPSECUSR                          Page/Line   1/1
Control . . . . .   _________                         Columns     1 - 78
Find  . . . . . .   ____________________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+...
                                                 User Profile Information
5770SS1 V7R2M0  140418
 Report type  . . . . . . . . . . :   *AUTINFO
 Select by  . . . . . . . . . . . :   *SPCAUT
 Special authorities  . . . . . . :   *ALL
                          -------------Special Authorities-------------
                                          *IO
 User         Group        *ALL   *AUD   SYS   *JOB   *SAV   *SEC   *SER   *SPL   User
 Profile      Profiles      OBJ    IT    CFG    CTL    SYS    ADM   VICE    CTL   Class
 CHENEY       *NONE         X      X      X     X      X      X      X      X     *SECOF
 JAMES        *NONE         X      X      X     X      X      X      X      X     *SECOF
 MN400OWN     *NONE                                                               *USER
 PAGERREXEC   *NONE                       X     X                                 *SYSOP
 PAGERUSR     *NONE                       X     X                                 *USER
 QANZAGENT    *NONE                                                               *SYSOP
 QAUTPROF     *NONE                                                               *USER
                                                                                 More...
```

common NETHERLANDS

Machtige gebruikersprofielen

- PRTUSRPRF command gebruiken om QPSECUSR spoolfile te bekijken

User Profile	Status	Not Valid Sign-ons	No Password	Local Password Management	Previous Sign-on
CHENEY	*ENABLED	0		*YES	11/04/17
DB2XML	*DISABLED	0	X	*YES	/ /
EMAIL	*DISABLED	1		*YES	12/10/07
FORGOT	*ENABLED	0		*YES	02/03/16
FTPMAN	*DISABLED	0		*YES	01/05/13
GARETH	*DISABLED	0		*YES	19/04/16
HAM400	*DISABLED	0	X	*YES	/ /
HELPDESK	*DISABLED	0	X	*YES	/ /
IJRN	*ENABLED	0	X	*YES	/ /
JAMES	*ENABLED	0		*YES	13/04/17
MDUNTITLED	*DISABLED	0	X	*YES	/ /
MN4000WN	*ENABLED	0	X	*YES	/ /
MRADMIN	*DISABLED	0	X	*YES	/ /

Machtige gebruikersprofielen

- PRTUSRPRF command gebruiken om QPSECUSR spoolfile te bekijken

Block Change	Password Expiration Interval	Password Changed	Password Expired
*SYSVAL	*NOMAX	11/03/14	*NO
*SYSVAL	*SYSVAL	21/07/11	*NO
*SYSVAL	*SYSVAL	08/04/15	*NO
*SYSVAL	*NOMAX	22/11/12	*NO
*SYSVAL	*SYSVAL	08/08/11	*NO
*SYSVAL	*SYSVAL	19/04/16	*NO
*SYSVAL	*SYSVAL	08/08/11	*NO
*SYSVAL	*NOMAX	08/08/11	*NO
*SYSVAL	*SYSVAL	04/03/15	*NO
*SYSVAL	*SYSVAL	05/01/17	*NO
*SYSVAL	*NOMAX	08/08/11	*NO
*SYSVAL	*SYSVAL	02/07/16	*NO
*SYSVAL	*NOMAX	08/08/11	*NO

Default Passwords

- ANZDFTPWD command gebruiken om een lijst van gebruikersprofielen met default wachtwoorden te bekijken(QPSECPWD)

```
                                        User profiles with default passwords.
5770SS1 V7R2M0  140418
 Action taken against profiles  . . . . . :   *NONE
 User
 Profile         STATUS          PWDEXP     Text
 TESTUSER        *ENABLED         *NO
                                    * * * * *   E N D   O F   L I S T I N
```

```
                                                User Profiles with Default Passwords
User                        Password  Profile   Last      Last         Special
Profile     Status          Expired   Created   Signon    Used         Authorities
            *ENABLED          *NO     03/05/93 26/04/16 26/04/16
            *ENABLED          *NO     27/10/10
            *ENABLED          *NO     03/10/13
            *ENABLED          *NO     10/03/11
```

common NETHERLANDS

Network Access Points

- Deactiveer wat je niet gebruikt
- Beperk gebruikers rechten voor reactivatie
  De *PUBLIC authority voor STRTCPSVR command mbt dit system is *EXCLUDE.
- Overweeg Exit Point applicaties om toegang te filtreren
- Commands kunnen uitgevoerd worden door LMTCPB users op bepaalde servers!
- NetServer Guest Profile

TCP/IP Server	Auto-Start Value
*SNMP	*NO
*ROUTED	*NO
*BOOTP	*NO
*TFTP	*NO
*DNS	*NO
*DHCP	*NO
*DDM	*YES
*TELNET	*YES
*FTP	*YES
*SMTP	*YES
*LPD	*YES
*POP	*YES
*REXEC	*NO
*HTTP	*NO
*DIRSRV	*YES
*NSLD	*NO
*INETD	*NO
*MGTC	*YES
*ONDMD	*NO
*NETSVR	*YES
*DLFM	*NO
*VPN	*NO
*EDRSQL	*NO
*HOD	*NO
*ODPA	*NO
*NTP	*NO
*QOS	*NO
*TCM	*NO
*DOMINO	*NO
*WEBFACING	*YES
*DEBUG	*NO
*ASFTOMCAT	*YES

Object Rechten

- Een ‘legacy’ probleem
- Het laatste obstakel
- Overweeg remediation en beheer te automatiseren
- Bekijk ook IFS Directories!
- Bekijk toegang tot objecten via de IFS File Shares
- Check QCRTAUT sysval en *LIBCRTAUT

Object Rechten

5/03/11 12:41:57 xxxxxxxxxxxxxxxxxx

SkyView Risk Assessor
Object Authorities

Library	Object Type	*ALL	*CHANGE	*USE	*EXCLUDE	*AUTL	USER DEF
xxxxx	*LIB		X				
	*CMD	0	0	0	0	0	0
	*PGM	0	0	0	0	0	0
	*FILE	0	0	0	0	0	0
xxxxxx	*LIB				X		
	*CMD	0	0	0	0	0	0
	*PGM	0	0	0	0	0	0
	*FILE	469	29	15	0	0	0
xxxxx	*LIB		X				
	*CMD	0	0	0	0	0	0
	*PGM	0	0	0	0	0	0
	*FILE	0	6	0	0	0	0
xxxxxx	*CMD	0	0	0	0	0	0
	*PGM	0	0	0	0	0	0
	*FILE	3	0	0	0	0	0

Adopted Authority

- Geeft gebruikers de rechten van de eigenaar van een programma
- Nodig voor sommige applicaties
- Voor “hackers” kan dit een ‘back door’ zijn
- PRTADPOBJ en analyseer output
- Overleg met de Application leverancier (als hij nog bestaat!)

Adopted Authority

5/03/11 12:42:44 xxxxxxxxxxxxxxxxxxxxx

SkyView Risk Assessor

Objects that Adopt *ALLOBJ Authority

User with *ALLOBJ	Object Adopting	Object Type	Text
x			
x			
QSECOFR	xxxxxxxxxxxxxxxxx	*PGM	x
QSECOFR	xxxxxxxxxxxxxxxxx	*PGM	x
QSECOFR	xxxxxxxxxxxxxxxxx	*PGM	x
QSECOFR	xxxxxxxxxxxxxxxxx	*PGM	x
QSECOFR	xxxxxxxxxxxxx	*PGM	x
QSECOFR	xxxxxxxxxxxxx	*PGM	x
QSECOFR	QGPL/QSTRUP	*PGM	x
QSECOFR	QGPL/Xxxxxxxx	*PGM	Adopt qsecofr rights

Wat vinden we

- Gebruikersprofielen met default wachtwoorden
- Groupprofiles! (e.g. QSECOFR)
- Te veel gebruikers met hoge rechten
- Limited Capabilities (nou en!)
- Zwakke object beveiliging
- Geen of beperkte auditing
- Adopted Authorities
- Service Tool (DST) Gebruikersprofielen met default wachtwoorden!
- Viruses?
- Enz enz

Remediation

- Creëer een Security Policy!
- Identificeer hoog, middel en laag risico’s
- Prioriteer
- Plan de remediation
- Analyseer en test de gevolgen
- Implementatie – in verschillende fases
- Herhaal!
- Automatiseren en/of outsourcen?

Vragen?

- Bedankt

common
NETHERLANDS