PRÄSENTIERT

Die 10 wichtigsten Schwachstellen, die Ihre IBM i angreifbar machen!

Stephan Leiße | Senior Sales Engineer
stephan.leisse@precisely.com

precisely

POW3R
einfach. digital. agil.

Schwachstelle Nr.10 – Es muss nichts getan werden

- Überzeugung, dass IBM i standardmäßig sicher ist
- "Wir vertrauen unseren Mitarbeitern"
- Keine Anforderungen an die Einhaltung von Vorschriften

precisely

..... die auf IBM i befindlichen Daten Sind für Ihr Unternehmen nicht wichtig?

precisely

Akteptieren, dass versehentliche Fehler vorkommen

Anwender mit internen Kenntnissen

- Böswillige Mitarbeiter - 14%
- Diebstahl von Zugangsdaten - 23%
- Nachlässigkeit - 63%

Ponemon Institute The Cost of Insider Threats – 2020

- https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

precisely

Schwachstelle Nr.9 – Einstellen und Vergessen

Sicherheitsprojekt wurde abgeschlossen oder ein Audit durchgeführt - kein Prozess zur Überprüfung vorhanden:

- Einstellungen der Benutzerprofile
  - Standard-Passwörter
  - Besondere Berechtigungen
  - Gruppenprofile Mitgliedschaft
  - Alte Profile
- Berechtigungseinstellungen
  - Bibliotheken, Verzeichnisse, Dateien
  - Berechtigungslisten
- Dateifreigaben
- TCP/IP-Einstellungen
  - Autostart-Werte, Verschlüsselungseinstellungen

precisely

Sicherheit ist kein einmaliges Ereignis…

Es ist ein Lebensstil !

precisely

Regelmäßige Überprüfung

Benutzerprofile

- Standard-Passwörter
  - ANZDFTPWD
- Spezielle Berechtigungen
  - PRTUSRPRF
- Gruppenprofile Zugehörigkeit
  - DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT)

Berechtigungseinstellungen

- Dateien
- Verzeichnisse
  - PRTPVTAUT OBJTYPE(*DIR) DIR('/Ihr Verzeichnis') SCHSUBDIR(*YES)
- Berechtigungslisten
  - PRTPVTAUT OBJTYPE(*AUTL) CHGRPTONLY(*YES)

precisely

POWER
einfach. digital. agil.

QSYS2.user_info - Special Authorities

```
11 SELECT authorization_name, special_authorities,
12 group_profile_name, supplemental_group_list, text_description FROM QSYS2.USER_INFO
13 WHERE SPECIAL_AUTHORITIES LIKE '%*ALLOBJ%'
14 OR AUTHORIZATION_NAME IN (
15 SELECT USER_PROFILE_NAME
16 FROM QSYS2.GROUP_PROFILE_ENTRIES
17 WHERE GROUP_PROFILE_NAME IN (
18 SELECT AUTHORIZATION_NAME
19 FROM QSYS2.USER_INFO
20 WHERE SPECIAL_AUTHORITIES like '%*ALLOBJ%'
21 )
22 )
23 ORDER BY AUTHORIZATION_NAME;
```

Authorization Name AUTHORIZATION_NAME	SPECIAL_AUTHORITIES			Group Profile Name GROUP_PROFILE_NAME	Supplemental Group List SUPPLEMENTAL_GROUP_LIST	Text Description TEXT_DESCRIPTION
AARONC	*ALLOBJ	*SECADM	*JOBCTL...	*NONE	-	-
ACADMN01	*ALLOBJ	*SECADM		*NONE	-	Admin user for aut

precisely

POWER
einfach. digital. agil.

Object Authority Services

QSYS2.object_privileges (DSPOBJAUT)

```
-- Permissions
-- Ownership
select * from qsys2.object_privileges where
system_object_schema = 'CWOODBURY' and
owner <> 'CWOODBURY';

-- *PUBLIC authority
select * from qsys2.object_privileges where
system_object_schema = 'CWOODBURY' and
authorization_name =   '*PUBLIC'   and
object_authority <>    '*EXCLUDE';
```

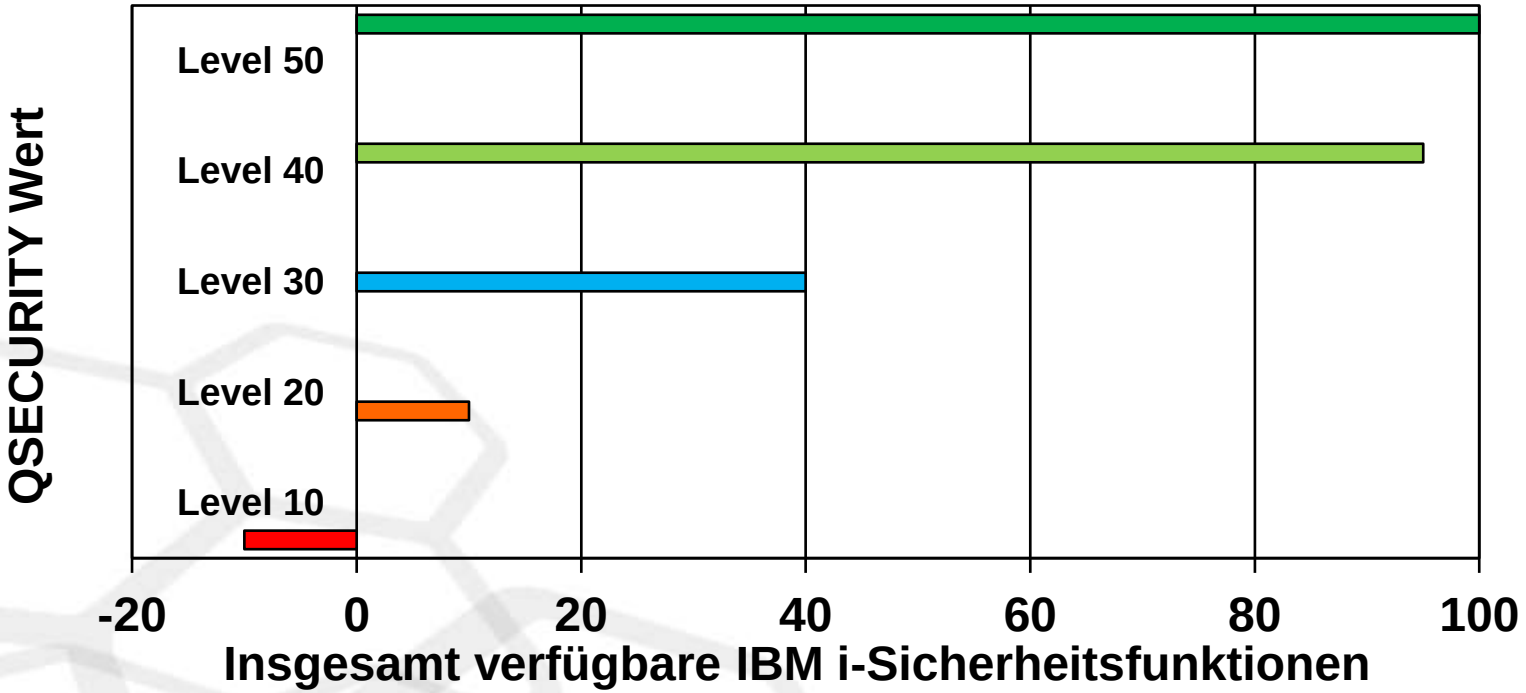
QSYS2.ifs_object_privileges (DSPAUT)

QSYS2.object_ownership (WRKOBJOWN / QSYLOBJA)

precisely

POWER
einfach. digital. agil.

Schwachstelle Nr. 8 - Betrieb mit falscher Sicherheitsstufe



Anfällig für:

- Ausführen von Batch-Jobs mit erhöhter Berechtigung
- Umgehung einiger Überprüfungen
- Direktes Aufrufen von OS-Programmen

Hinweis: Die Berechtigungen beim Erstellen von Profilen umfassen *ALLOBJ und *SAVSYS (Level 20)

precisely

POWER
einfach. digital. agil.

Wechsel zu einer höheren Sicherheitsstufe

Umstellung von 30 auf 40/50:

- Muss geprüft werden, um Probleme zu ermitteln (falls vorhanden)

Umstellung von 20 auf 40/50

- Viel mehr Planung erforderlich

Weitere Details sind hier zu finden:

IBM i Security Reference, Kapitel 2

- IBM i Security Administration and Compliance, 3rd edition

precisely

POWER
einfach. digital. agil.

Schwachstelle Nr. 7 - Kein Passwort für DDM erforderlich

- Ein Attribut des DDM-Servers bestimmt, ob auf dem Zielsystem ein Passwort erforderlich ist
- Mit ADDSVRAUTE kann ein Benutzer festlegen, dass er als ein anderes Profil auf dem Zielsystem läuft - einschließlich QSECOFR

```
                    Add Server Auth Entry (ADDSVRAUTE)

Type choices, press Enter.

User profile . . . . . .   cjw          Name, *CURRENT
Server . . . . . .         QDDMSERVER
_____
User ID  . . . . . .       QSECOFR_
_____
User password  . . . . . .  *NONE
_____
```

precisely

POWER
einfach. digital. agil.

Absicherung von DDM

- Untersuchen Sie, welche Profile DDM verwenden, *bevor* Sie die Serverattribute so ändern, dass ein Passwort erforderlich ist!
  - Verwenden Sie die **GR** Audit-Journal Einträge und suchen Sie nach der Verwendung von DDM/DRDA.
  - Sehen Sie sich die Exit-Point-Protokolle an

- Fügen Sie für jedes Profil, das DDM verwendet, einen Eintrag zur Serverauthentifizierung hinzu

- Verwendung eines Gruppenprofils für den DDM-Zugriff
  - https://www.ibm.com/support/pages/simplified-ddm-and-drda-authentication-entry-management-using-group-profiles

- Passwort des aktuellen Benutzers für DDM-Zugang verwenden
  - https://www.ibm.com/support/pages/enable-drda-and-ddm-authentication-using-user-profiles-password

precisely

POW3R
einfach. digital. agil.

Absicherung von DDM – Teil II

- ADDSVRAUTE auf *PUBLIC *EXCLUDE setzen
- Setzen Sie QSECOFR auf STATUS(*DISABLED)
- Verwenden Sie die Anwendungsverwaltung, um den Zugriff abzuschalten
- Verwenden Sie eine Exit Point-Software, um den Zugriff zu protokollieren und zu kontrollieren

Schwachstelle Nr. 6 - Alte Sachen aufbewahren

- Inaktive Profile
- Archivierte Daten nach dem Aufbewahrungsplan
- Kopien die vor einer Aktualisierung der Datenbank erstellt wurden
  - DateinameX, DateinameAlt, Dateiname2, DateinameKopie
- Außer Betrieb gesetzte Server
- Frühere Versionen von Herstellerprodukten
- Nicht mehr genutzte Herstellerprodukte
- Dateifreigaben

precisely

Profile bleiben mit Zugriff erhalten

- Auch wenn Benutzer (Mitarbeiter / Externe Dienstleister) die Organisation verlassen haben, bleibt ihr Zugriff bestehen
- MUSS einen Prozess existieren, der sicherstellt dass der Zugriff sofot beendet wird
  - Vergessen Sie nicht die SAAS-Anwendungen - Gehaltsabrechnung/HR, CRM, etc.

Benutztung von:

- CHGUSRPRF auf *DISABLE zu einem bestimmten Datum oder Zeitrahmen (Tage)
- GO SECTOOLS
  - Option 8 zum *DISABLE oder *DELETE an einem bestimmten Datum
- WRKOBJOWN oder QSYS2.object_ownership, um Eigner Objekte zu finden

precisely

POWER
einfach. digital. agil.

Schwachstelle Nr. 5 - Sitzungen sind nicht verschlüsselt

- Interne Kommunikation ist oft nicht verschlüsselt
- WFH oder WFS (Work from Starbucks) ohne Verwendung eines VPN

- Anfällig für Sniffing

precisely

Sitzungen verschlüsseln

- Beziehen Sie ein digitales Zertifikat von einer bekannten CA (Certificate Authority) oder konfigurieren Sie die IBM i als CA
  - https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzahu/rzahurazhudigitalcertmngmnt.htm
  - http://IBM_I:2006/dcm/login
- Verwenden Sie den SST-Befehl SSLCONFIG oder TLSCONFIG (V7R4), um festzustellen, welche Protokolle verwendet werden
  - https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzain/rzainhscounter.htm
- Verwenden Sie *NETSCK, *NETUDP und *NETTELSVR in QAUDLVL, um festzustellen, ob eine unsichere Kommunikation verwendet wird (V7R3)
  - https://www.mcpressonline.com/security/ibm-i-os400-i5os/how-can-i-tell-whether-all-the-connections-to-my-ibm-i-are-secure

precisely

POWER
einfach. digital. agil.

Schwachstelle Nr. 4 - Daten sind nicht geschützt

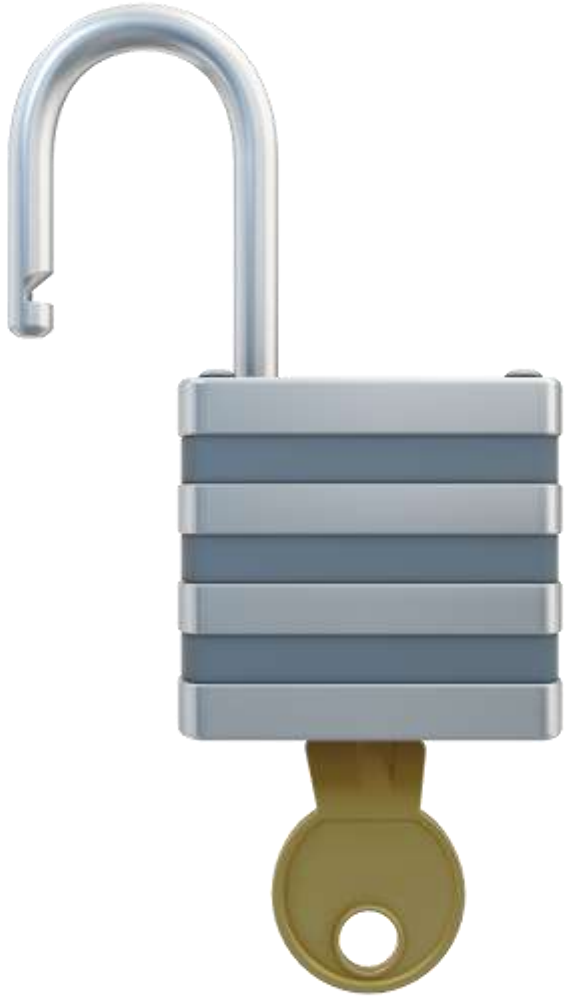
Die Daten sind nicht geschützt gegen:

- versehentliche Änderung
- versehentliches (oder absichtliches) Löschen
- Herunterladen durch Einzelpersonen ohne geschäftliche Rechtfertigung

precisely

Wie / Warum passiert das?

- Denkweise dass Objektsicherheit zu schwierig ist
- IFS wird ignoriert
- Die Unternehmensdaten einer Organisation werden ignoriert
- Den Mitarbeitern ist nicht klar, wo sich (alle) die Daten befinden



precisely

Mehrere Verteidigungsschichten / Defense in Depth

- Objektsicherheit
  - NICHT alles oder nichts!
  - Authority Collection – verfügbar ab V7R3 und erweitert in V7R4
- Maskierung und/oder zusätzliche Berechtigungen über Row and Column Access Control (RCAC)
- Verschlüsselung über FIELDPROC
- Exit-Point-Software

Implementieren Sie so viele Verteidigungsschichten, wie erforderlich sind, um das Risiko auf ein akzeptables Niveau zu reduzieren

precisely

Schwachstelle Nr. 3: Kein Einblick was auf IBM i passiert

- ✓ Kein Auditing aktiviert oder nie überprüft
- ✓ Informationen zur Sicherheit werden nicht an das evtl. vorhandene SIEM gesendet

precisely

Audit-Empfehlungen

QAUDCTL

- *OBJAUD
- *AUDLVL
- *NOQTEMP (optional)

QAUDLVL

- *AUTFAIL
- *PGMFAIL (nur bei Änderung von 20/30 zu 40/50)
- *CREATE
- *DELETE
- *PTFOPR, *PTFOBJ
- *SAVRST
- *SECCFG and *SECRUN (oder *SECURITY)
- *SERVICE

- *OBJMGT
- *JOBBAS (erzeugt eine MENGE Einträge)
- *ATNEVT (Intrusion Detection auf IP-Stack-Ebene)

precisely

SIEM (Security Information and Event Management)

- Senden Sie IBM i-Ereignisse an Ihr SIEM (oder SYSLOG Server)?
  - Wenn nicht, warum nicht?
- Wofür wird Ihr SIEM verwendet?
  - System zur Aufzeichnung oder zur Erkennung unangemessener Aktivitäten

Siehe MC Press Artikel für weitere Überlegungen:

- https://www.mcpressonline.com/security/ibm-i-os400-i5os/what-ibm-i-information-should-i-be-sending-to-my-siem

precisely

POWER
einfach. digital. agil.

Senden von Audit-Einträgen an das SIEM

- **PW**
  - 'U'-Einträge, bei denen der Benutzer "root" oder "Admin" ist und der Versuch von außerhalb der Organisation stammt
  - P"-Einträge, bei denen viele innerhalb eines kurzen Zeitraums und für die bekannten, von IBM i bereitgestellten Profile (QSYS, QSECOFR, QUSER, QSYSOPR, QPGMR, QSRV, QSRVBAS) auftreten
- **JS**
  - Job Start Einträge von einer unbekannten externen IP-Adresse
  - Job startet für unbekannte Einträge (z. B. QSECOFR)
- **CP**
  - Passwortänderungen für QSECOFR und andere von IBM gelieferte Profile
  - Wiederfreigabe von QSECOFR (wenn STATUS *DISABLED gehalten wird)

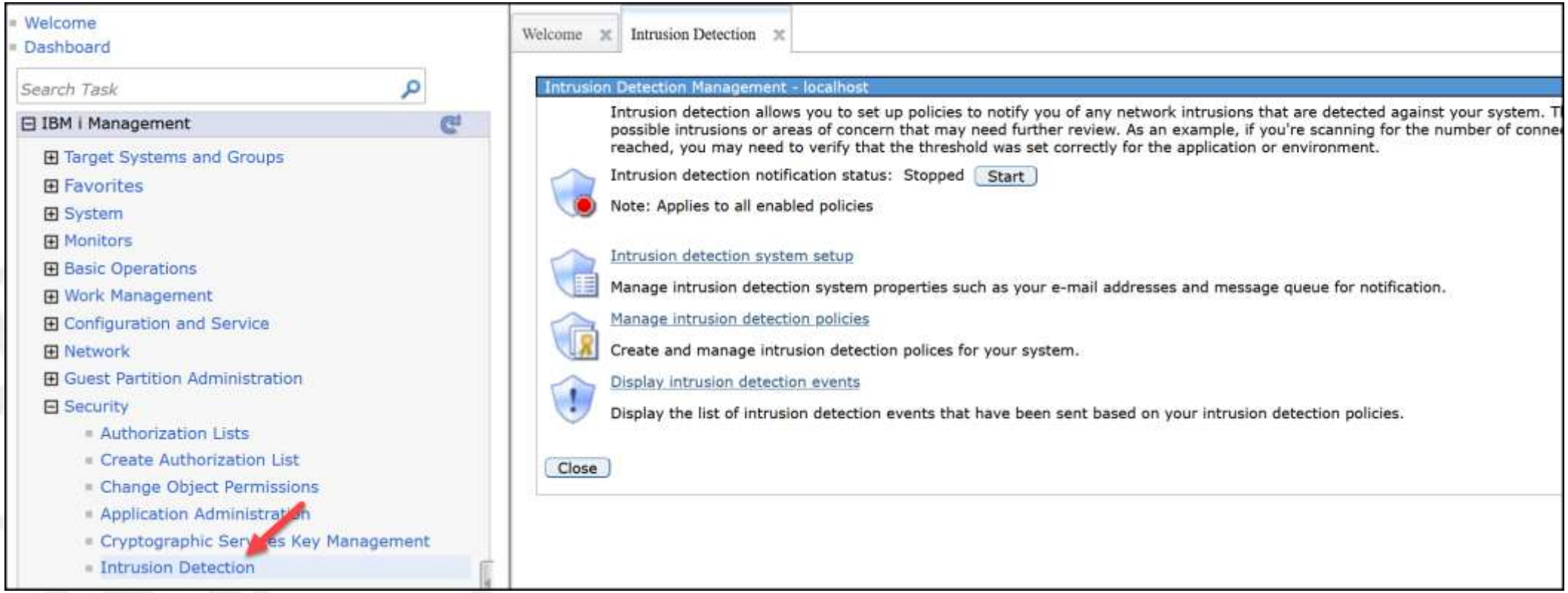
Weitere Details:

https://www.mcpressonline.com/security/ibm-i-os400-i5os/what-ibm-i-information-should-i-be-sending-to-my-siem

precisely

POWER
einfach. digital. agil.

Verwendung von Intrusion Detection



IM - Audit-Einträge - Dient zur Erkennung von DDoS-Angriffen und Cryptomining-Malware
Siehe: https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzaub/rzaubkickoff.htm

precisely

POWER
einfach. digital. agil.

Schwachstelle Nr. 2: Authentifizierung

- Falsch eingestellter Passwort Systemwert
- Zulassen von schwachen Kennwörtern (einschließlich Standardkennwörtern)
- Keine Multi-Faktor-Authentifizierung (MFA)
- Ausfüllen von Anmeldeinformationen

precisely

Password Level (QPWDLVL)

System value	
0	Standard Zeichensatz: A-Z, 0-9, $, @, # und _ Maximale Länge: 10
1	Gleich wie Level 0, aber das alte NetServer-Kennwort wird entfernt. **Unbedenklich wenn NetServer nicht verwendet oder keine Verbindung mit Windows 95, 98, ME oder Windows 2000 Server herstellen - Endbenutzer sehen keinen Unterschied**
2	Zeichensatz: Groß-/Kleinschreibung, alle Interpunktions- und Sonderzeichen, Zahlen und Leerzeichen Maximale Länge: 128 Behält das NetServer-Passwort bei, verschlüsselt mit altem und neuem Algorithmus Anmeldebildschirm geändert, um längere Passwörter zu ermöglichen, CHGPWD und CRT/CHGUSRPRF pwd-Feld geändert
3	Wie Stufe 2, beseitigt das alte verschlüsselte Passwort und das alte NetServer-Passwort **Sicheres Verschieben, wenn Sie NetServer nicht verwenden oder keine Verbindung mit Windows 95, 98, ME oder Windows 2000 Server herstellen - Endbenutzer sehen keinen Unterschied**

Hinweis: Änderungen erfordern eine IPL
Erst zum Wert 2, bevor 3 verwendet wird. Mit Wert 2 kann ein Passwort verwendet werden, das in GROSSBUCHSTABEN oder in kleinbuchstaben geschrieben ist, bis es geändert wird. **Anwender müssen geschult werden!**

precisely

System Werte des für das Anmelden

System value	Recommended setting
QMAXSIGN	3-5
QMAXSGNACN	2 (Deaktivieren des Profils) oder 3 (Deaktivieren des Profils und des Geräts)

precisely

POWER
einfach. digital. agil.

Passwort-Zusammensetzungsregeln (WRKSYSVAL QPWD*)

precisely

POWER
einfach. digital. agil.

QPWDRULES

*PWDSYSVAL oder

- *CHRLMTAJC
- *CHRLMTREP
- *DGTLMTAJC
- *DGTLMTFST
- *DGTLMTLST
- *DGTMAXn
- *DGTMINn
- *LMTSAMPOS
- ***LMTPRFNAME**
- *LTRLMTAJC
- *LTRLMTFST
- *LTRLMTLST
- *LTRMAXn
- *LTRMINn

- ***MAXLENnnn**
- ***MINLENnnn**
- *MIXCASEnnn
- ***REQANY3**
- *SPCCHRLMTAJC
- *SPCCHRLMTFST
- *SPCCHRLMTLST
- *SPCCHRMAXn
- *SPCCHRMINn

V7R2

- ***ALLCRTCHG**

→ Empfohlen: Regeln sind alle an einem Ort, mehr Optionen

Hinweis: ALLE Regeln müssen in QPWDRULES abgelegt werden, sobald sie von der Standardeinstellung geändert wurden.

precisely

Standard-Passwörter

- Festlegen von *LMTPRFNAME und *ALLCRTCHG in QPWDRULES
  - Die Einstellung, dass das Passwort bei der ersten Anmeldung geändert werden muss, ist kein Schutz!

- Führen Sie ANZDFTPWD aus, um zu ermitteln welches Benutzerprofil = Passwort hat

Credential Stuffing

- Verwendung von zuvor gestohlenen/kompromittierten Anmeldeinformationen (Benutzer-ID und Kennwörter), um zu versuchen, Zugang zu einer anderen Website oder Organisation zu erhalten.

- Verwenden Sie Passwörter NICHT wieder!!!

precisely

POW3R
einfach. digital. agil.

Multi-factor Authentication (MFA)

- Erfordert zwei oder mehr "Faktoren", um sich zu authentifizieren (Zugang zum System zu erhalten)
  - Etwas, das Sie wissen (Passwort, Pin)
  - Etwas, das Sie sind (Fingerabdruck, Gesichtserkennung, optischer Scan)
  - Etwas, das Sie haben (Token, Bankkarte)
- Empfohlen für mindestens Benutzerprofile mit hohen Berechtigungen
- Hilft ‚Credential Stuffing' zu verhindern

precisely

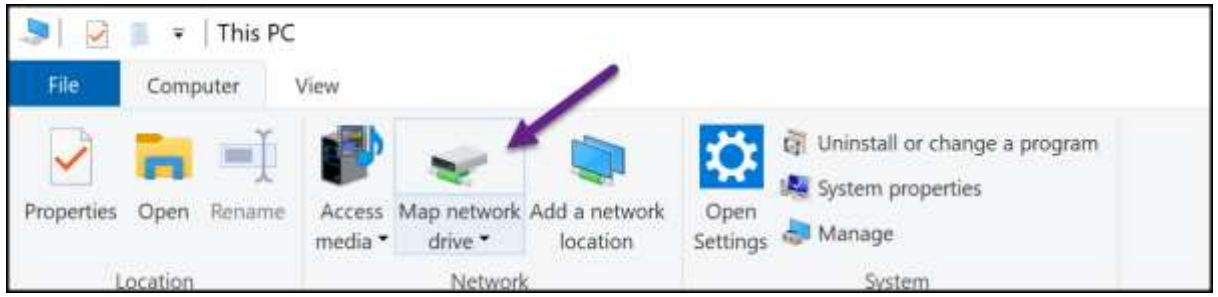
POWER
einfach. digital. agil.

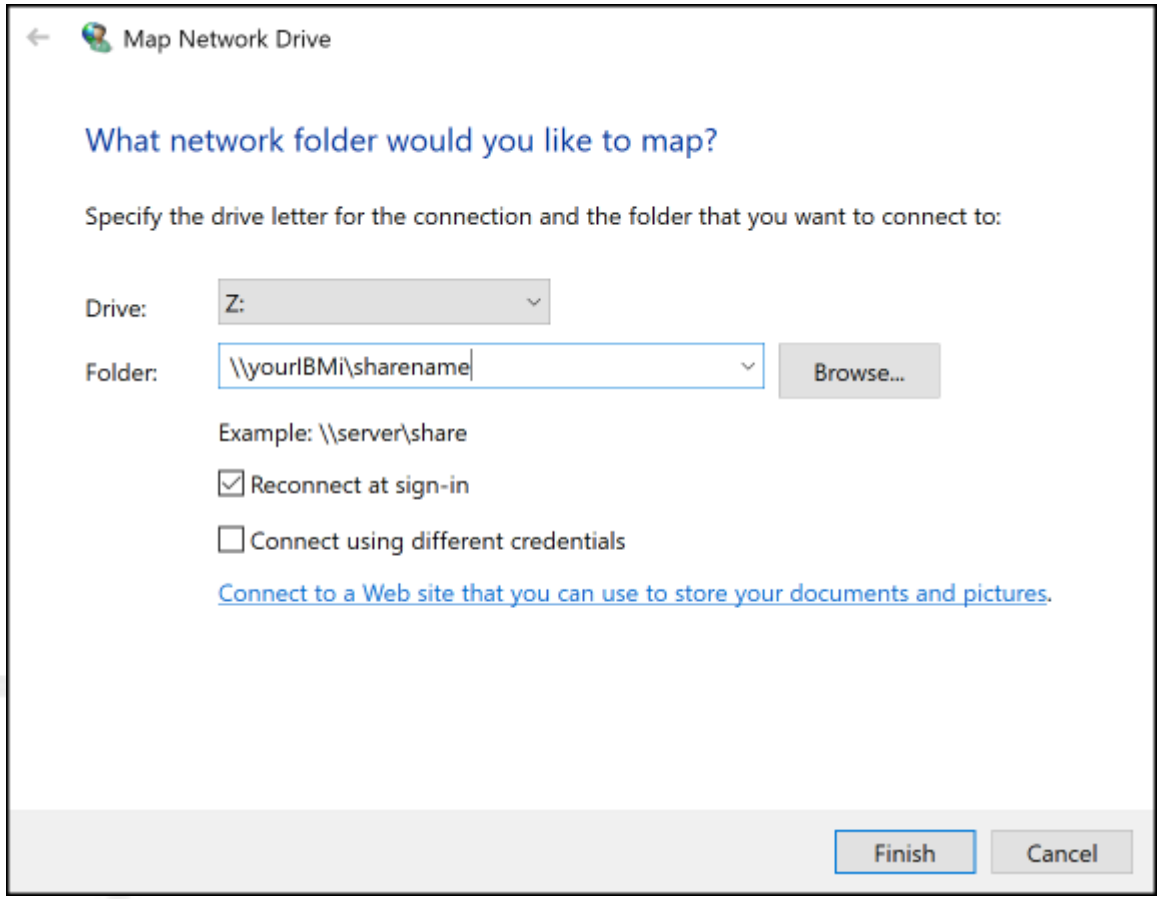
Schwachstelle #Nr.1: Malware

Zwei Arten von Malware betreffen die IBM i:

- Resident (gespeichert) im IFS
- Über eine Dateifreigabe eintreffend

precisely


This PC
File
Computer
View
Properties
Open
Rename
Location
Access media
Map network drive
Add a network location
Network
Open Settings
Uninstall or change a program
System properties
Manage
System


Map Network Drive
What network folder would you like to map?
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
Z:
Folder:
\\yourIBMi\sharename
Browse...
Example: \\server\share
Reconnect at sign-in
Connect using different credentials
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

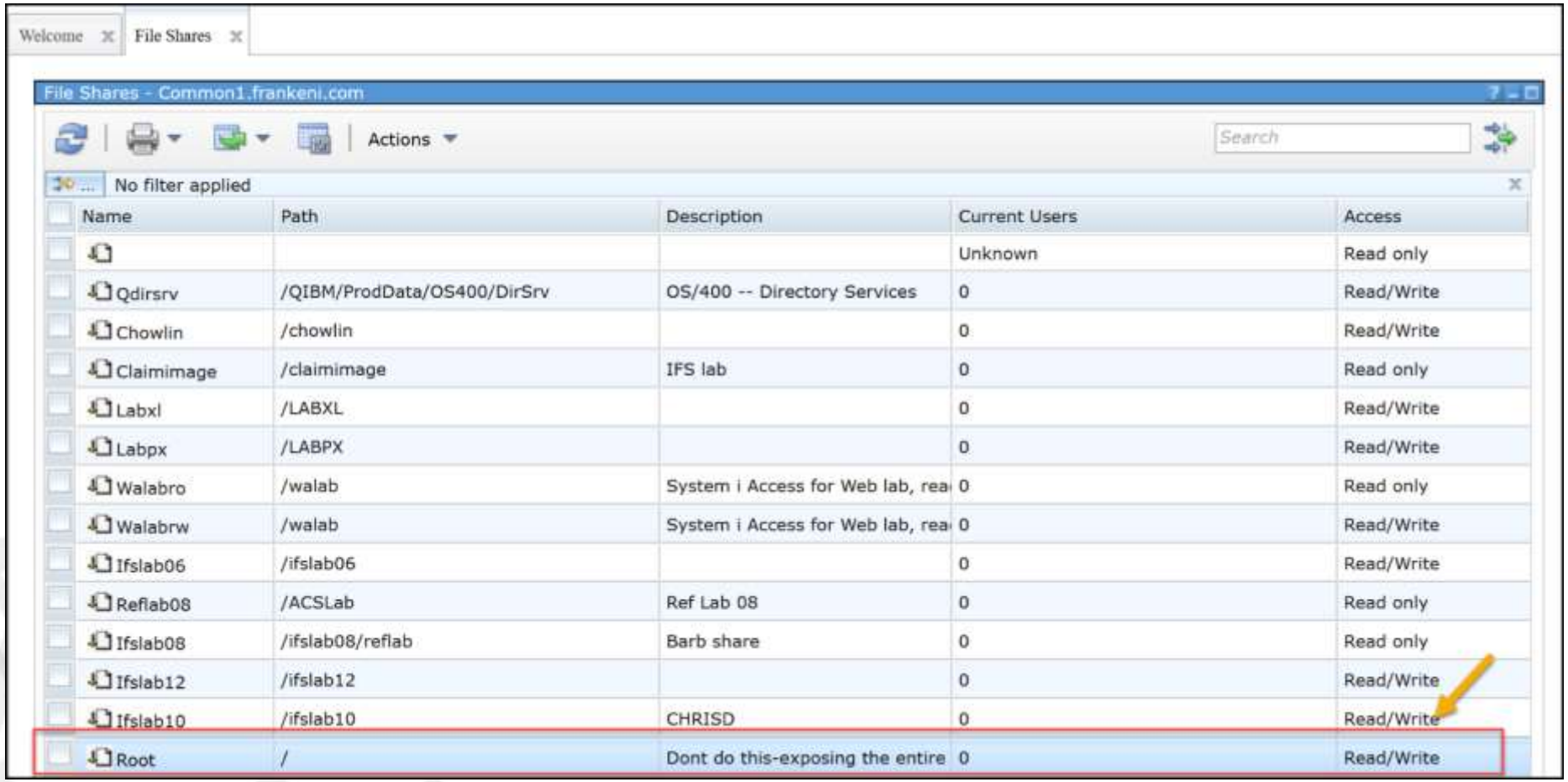
precisely

*ALLOBJ und Verzeichnisberechtigungen

- Im Gegensatz zu Windows gibt es keine Berechtigung auf der Freigabe selbst
- Was die Malware tun kann, hängt davon ab
  - Wie die Freigabe definiert ist - nur lesen oder lesen/schreiben
  - Die Berechtigung des Benutzers für das Verzeichnis und die Objekte im Verzeichnis

Datei-Freigaben

Das Worst-Case Szenario ist eine Lese-/Schreibfreigabe für root

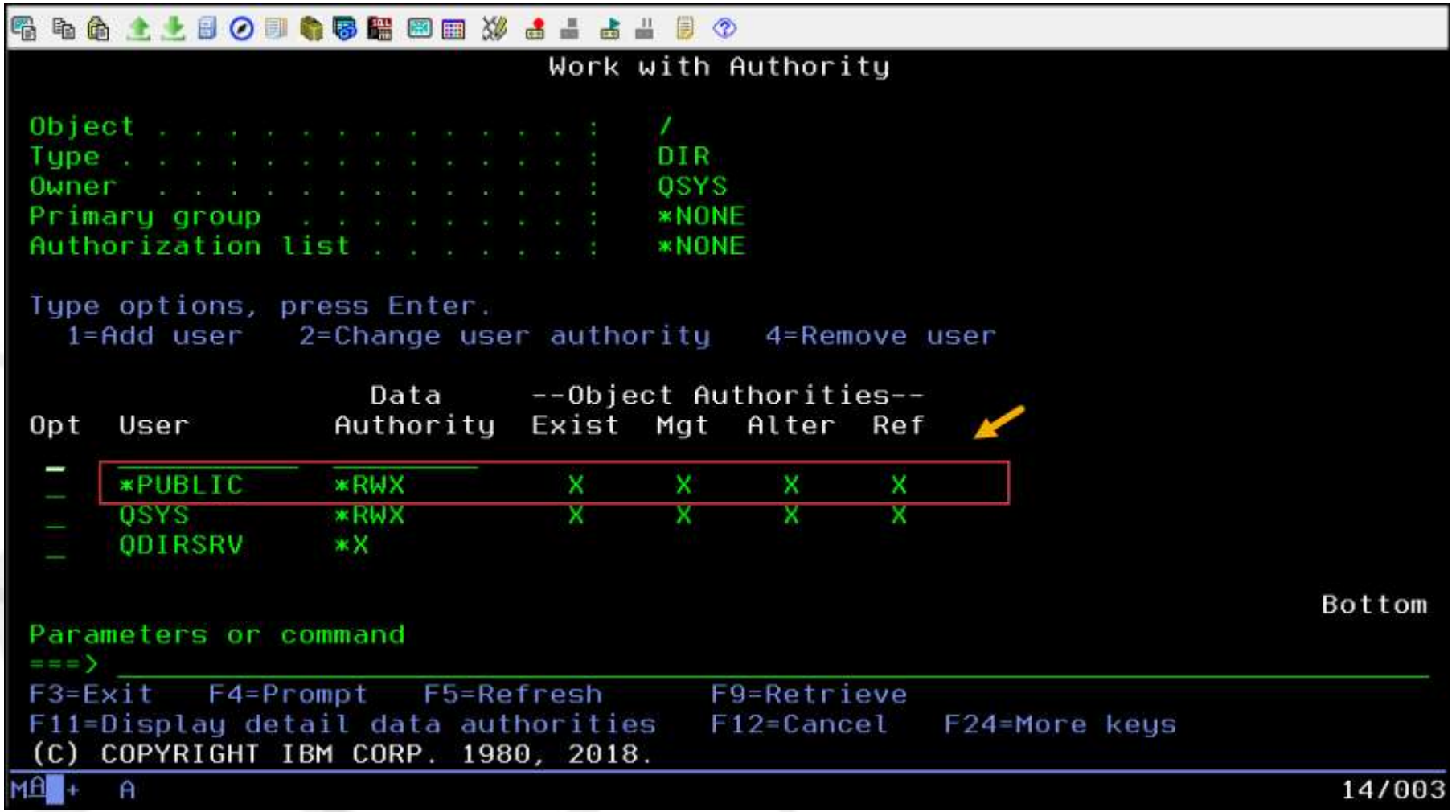


Name	Path	Description	Current Users	Access
			Unknown	Read only
Qdirsrv	/QIBM/ProdData/OS400/DirSrv	OS/400 -- Directory Services	0	Read/Write
Chowlin	/chowlin		0	Read/Write
Claimimage	/claimimage	IFS lab	0	Read only
Labxl	/LABXL		0	Read/Write
Labpx	/LABPX		0	Read/Write
Walabro	/walab	System i Access for Web lab, rea	0	Read only
Walabrw	/walab	System i Access for Web lab, rea	0	Read/Write
Ifslab06	/ifslab06		0	Read/Write
Reflab08	/ACSLab	Ref Lab 08	0	Read only
Ifslab08	/ifslab08/reflab	Barb share	0	Read only
Ifslab12	/ifslab12		0	Read/Write
Ifslab10	/ifslab10	CHRISD	0	Read/Write
Root	/	Dont do this-exposing the entire	0	Read/Write

precisely

POWER
einfach. digital. agil.

Verzeichnisberechtigungen



Empfohlene *Berechtigung für root:
DTAAUT(*RX)
OBJAUT(*NONE)

precisely

POWER
einfach. digital. agil.

Risiko von Malware reduzieren

- Schulen Sie Ihre Anwender!
- Backups
  - Durchführen!
  - Überprüfen der Sicherungen!
  - Separat aufbewahren

- *Freigaben*
  - ***ROOT NICHT FREIGEBEN !!!! (oder QSYS.lib)***
  - *Entfernen Sie unnötige Freigaben*
  - *Setzen Sie Freigaben auf Read-only, wenn möglich*
  - *Verstecken Sie Freigaben, indem Sie sie mit einem '$' erstellen - z. B. newshare$*
  - *Schalten Sie das Broadcasting des NetServers aus*

precisely

POW3R
einfach. digital. agil.

Risiko von Malware reduzieren Teil II

- Berechtigungen
  - Nach der Überprüfung, setzen Sie root auf DTAAUT(*RX) OBJAUT(*NONE)
  - Überprüfen Sie kritische Pfade und schränken Sie den Zugriff gegebenenfalls ein
    - Ransomware hat begonnen, die Daten zu filtern und droht, sie zu veröffentlichen
  - Überprüfen Sie, wer die Sonderberechtigung *ALLOBJ hat
- Beenden Sie Programme
  - Wenn Sie Exit-Point-Software haben, verwenden Sie den NetServer Exit Programm, um zu kontrollieren, welche Profile nutzen können
- Berücksichtigen Sie die Netzwerksegmentierung

precisely

POWER
einfach. digital. agil.

Wenn infiziert ...

Holen Sie Ihren Notfallplan heraus!

- Feststellen ob Sie noch angegriffen werden oder ob der Angriff eingedämmt ist
- Feststellen ob Sie den Vorfall selbst beheben können oder ob Sie Experten hinzuziehen müssen
- Feststellen ob Sie die Strafverfolgungsbehörden benachrichtigen müssen
- Falls Ransomware, entscheiden ob Lösegeld gezahlt werden soll oder nicht

Qualität und Verfügbarkeit Ihrer Backups können darüber entscheiden, ob Sie sich von einem Malware-Angriff erholen können

precisely

POW3R
einfach. digital. agil.

Fragen?
Antworten!

precisely

POW3R
einfach. digital. agil.

PRÄSENTIERT

Die 10 wichtigsten Schwachstellen, die Ihre IBM i angreifbar machen!

Stephan Leiße | Senior Sales Engineer
stephan.leisse@precisely.com

precisely

POW3R
einfach. digital. agil.