

infor



70. Anwendertreffen

13./14. November 2025

Vienna House by Wyndham Ernst Leitz
Wetzlar



1

infor

IT Sicherheit

Praktische IT Sicherheit im Zusammenhang mit COM

Christoph Marschibois
Technische Beratung

Datum 14.11.2025

INDUSTRY SPECIFIC

COM SUITE SOLUTIONS

Copyright © 2025. Infor. All Rights Reserved. infor.com

2

IT Sicherheit – Definition



Sicherstellung von

Verfügbarkeit	Zugänglich bei Bedarf
Integrität	Daten sind korrekt und unverändert
Vertraulichkeit	Schutz vor unbefugtem Zugriff

Sicherheit ist kein Zustand sondern eine Prozess!



Copyright © 2025. Infor. All Rights Reserved. infor.com

3

IT Sicherheit - Bedrohungen

Insiderbedrohungen

Physische Gefahren

Physisches Hacking

Phishing und Social

Human Error

Malware

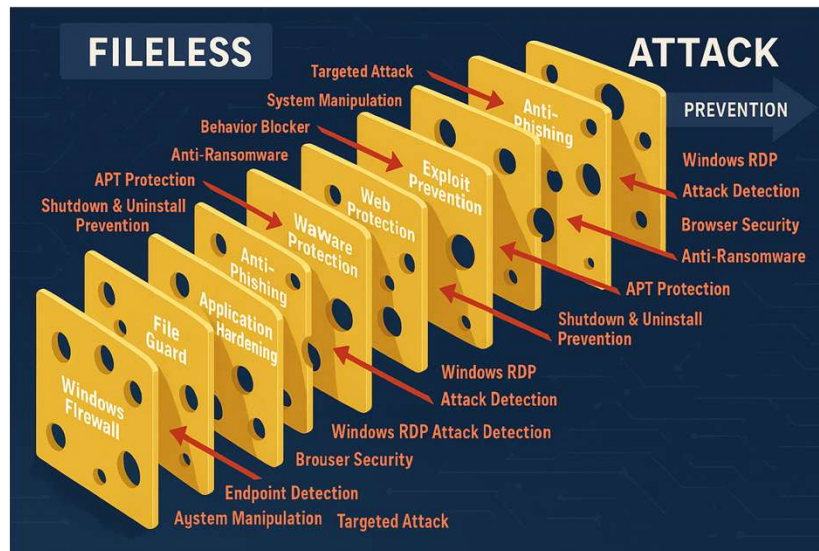
Hacker



Copyright © 2025. Infor. All Rights Reserved. infor.com

4

IT Sicherheit als Schweizer Käse

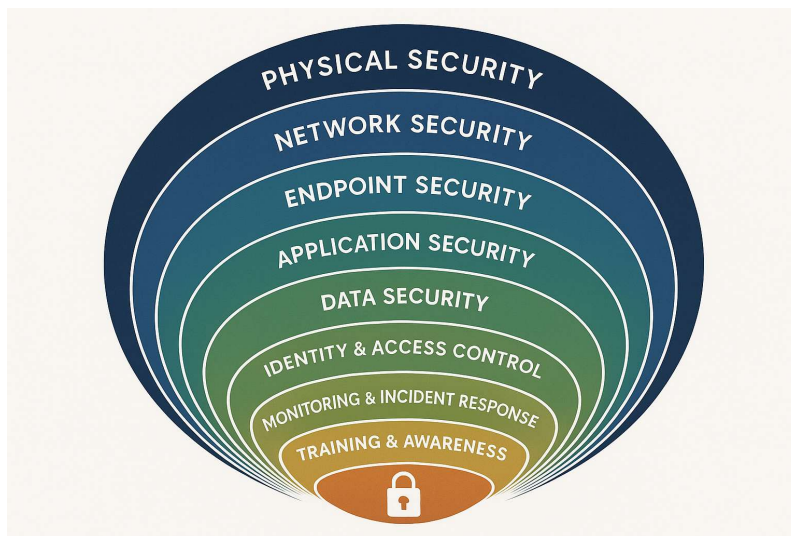


infor

Copyright © 2025. Infor. All Rights Reserved. infor.com

5

Layered Security Model



infor

Copyright © 2025. Infor. All Rights Reserved. infor.com

6

IT Sicherheit – Technische Maßnahmen



Firewalls



Zugriffsmanagement



Backup-Systeme



Netzwerksegmentierung

infor

Copyright © 2025. Infor. All Rights Reserved. infor.com

7

IT Sicherheit – Organisatorische Maßnahmen



Notfall- und
Wiederherstellungspläne:
Ablaufpläne für den Umgang
mit Sicherheitsvorfällen.

infor

Copyright © 2025. Infor. All Rights Reserved. infor.com

8

Was tun? Backups!

Das beste Backup ist das,
das man nicht braucht.

Regelmäßig

Woanders

Mehrfach

Automatisch

Versioniert

Dokumentiert

Überwacht

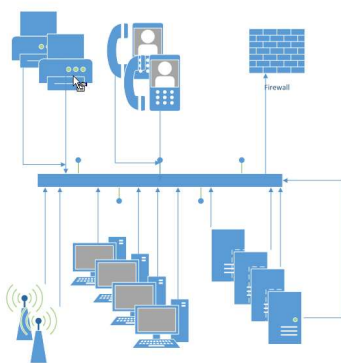
Getestet

infor

Copyright © 2025. Infor. All Rights Reserved. infor.com

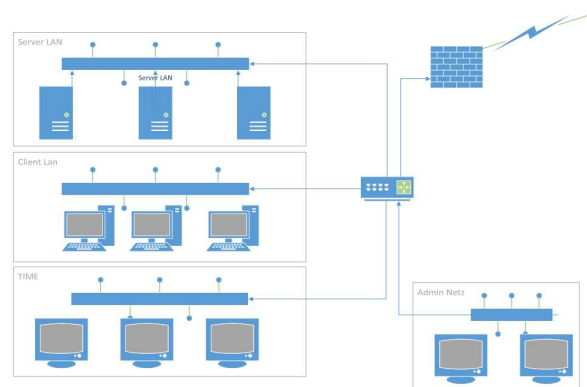
9

Was tun? Divide et impera! Netzwerksegmentierung



Switching OSI Layer 2
Sicherungsschicht
MAC

infor



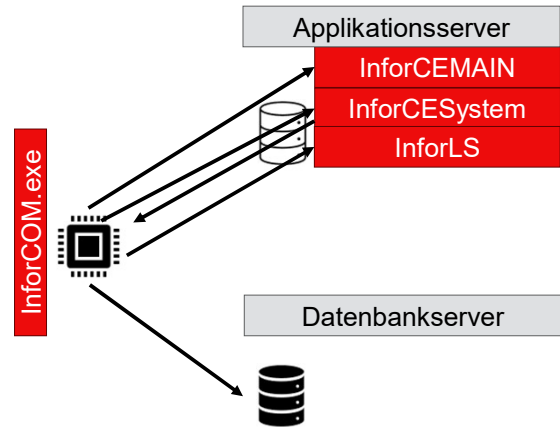
Firewall OSI Layer 4
Transportschicht
IP/Ports

Copyright © 2025. Infor. All Rights Reserved. infor.com

10

Infor COM und die Firewall

1. Infor COM baut Verbindungen zum InforCEMain auf und erhält die vorhandenen Systeme
2. Infor COM baut Verbindung zum SystemCE auf
3. Der InforCE des Systems baut eine Verbindung zum laufenden Infor COM auf
4. Infor COM verbindet sich zur Datenbank
5. Infor COM verbindet sich zum Lizenzserver



infor

Copyright © 2025, Infor. All Rights Reserved. infor.com

11

Netzwerkverbindungen der InforCOM.exe

inforCOM.exe:11616 Properties

Image Performance Performance Graph GPU Graph Threads TCP/IP Security Environment Job Strings

☒ Resolve addresses

Prot...	Local Address	Remote Address	State
TCP	59096	Client 59095	ESTABLISHED
TCP	59095	DB Server 59096	ESTABLISHED
TCP	59099	App Server 1521	ESTABLISHED
TCP	59138	Client 1521	ESTABLISHED
TCP	59097	App Server 5302	ESTABLISHED
TCP	59116	App Server 50608	ESTABLISHED
TCP	59098	Client 51684	ESTABLISHED
TCP	59098	Client 0	LISTENING

infor.com

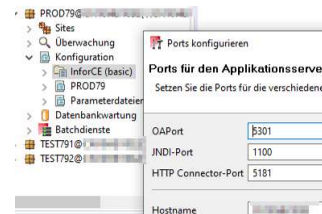
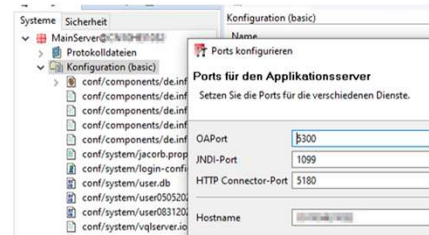
12

Ports auf dem Applikationsserver

Ports auf dem Applikationsserver, die von den Clients erreichbar sein müssen:

- InforCEMAIN
 - (Typisch 5300, 1099, 5180)
- InforCE Ports eines jeden System
 - PROD 5301, 1100, 5181
 - TEST1 5302, 1101, 5182
 - TEST2 5302, 1101, 5182
- Ports in der real existierenden Konfiguration nachschauen
- Lizenzserverport ist ab 7.7 Build 32423 fest einstellbar. siehe KB3637776 + KB2097806

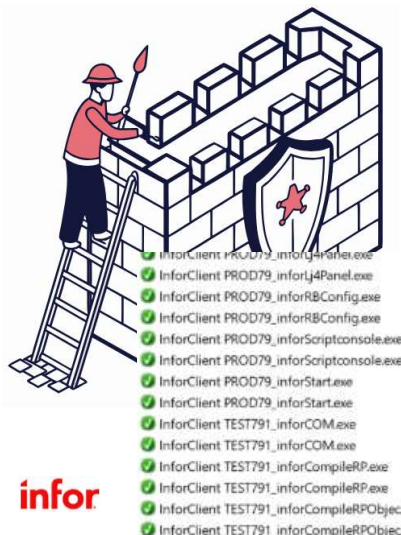
Inforconfig.ini
Parameter InforLicenceServicePortOptions=6300/portspan=1



Copyright © 2025, Infor. All Rights Reserved. infor.com

13

Regeln für die Windowsfirewall am Client



COM executables Incoming für das Profil "domain" sowohl für den Hostname als auch den FQDN eingeschaltet.

Zusätzlich zur inforcom.exe noch

inforCompileRP.exe, inforDM.exe, inforCompileRPObjec.exe, inforStart.exe, inforComponentInstaller.exe, inforLj4Panel.exe, inforScriptconsole.exe

Automatisiert mittels GPO,CMD,Powershell

Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforLj4Panel.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforLj4Panel.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforRBConfig.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforRBConfig.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforScriptconsole.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforScriptconsole.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforStart.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\PROD79\inforStart.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\TEST791\inforCOM.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\TEST791\inforCOM.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\TEST791\inforCompileRP.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\TEST791\inforCompileRP.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\TEST791\inforCompileRPObjec.exe	Allow	Yes
Domain	\\euce1wcom2\infor.com\infor795\inforcom\TEST791\inforCompileRPObjec.exe	Allow	Yes

14

Was tun? Divide et impera pars duo! Berechtigungen

Least Privilege Prinzip

Berechtigungen immer an Gruppen

Gruppennamen nach Konvention erstellen

Rechtevergabe auf hoher Hierarchieebene

Freigabe/NTFS Berechtigungen kombinieren

Überprüfen und Auditieren



Copyright © 2025. Infor. All Rights Reserved. infor.com

15

Berechtigungen infor\$ Freigabe



Verzeichnisbaum ist leider sehr tief; „Jeder darf alles“ Ansatz generell gefährlich und auch hier nicht zu empfehlen

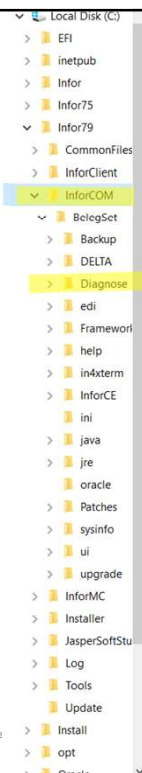
Nutzen Sie Domänengruppen

- GRP_INFORCOM_ADMIN
- GRP_INFORCOM_Keyuser (optional)
- GRP_INFORCOM_User

Leseberechtigungen für User sind nur auf das InforCOM System Verzeichnis und dessen Unterordner notwendig

Schreibberechtigungen für User sind im Standard nur auf das Diagnoseverzeichnis notwendig.

Bei höheren Securityanforderungen kann eine zusätzliche Freigabe inforCOM\$ genutzt werden



Copyright © 2025. Infor. All Rights Reserved. infor.com

16

Dateibasierte Schnittstellen



infor

DFS nutzen

- Dabei zeigt ein Pointer in der Domäne auf einen beliebigen Fileserver. Kann einfach von A nach B umgeschaltet werden

Eigene Freigabe für sensibles.

Vorteile:

- Übersichtlich
- saubere Berechtigungen lassen sich transparent und einfach vergeben
- Separate Verzeichnisse für PROD und TEST
- Anpassungen nur auf der sich ändernden Seite notwendig

Beispiele

- \\domain\Schnittstellen\Säge\PROD
- \\domain\Schnittstellen\Säge\TEST
- \\domain\SchnittstellenFIBU\SFIRM

Copyright © 2025. Infor. All Rights Reserved. infor.com

17

Das kann man so machen, das ist dann aber...



Arbeiten Sie nie mit dem User
Domäne\Administrator



Arbeiten Sie so wenig wie möglich mit
Domänenadminberechtigungen



Melden Sie sich ausschließlich auf aktuellen
Systemen mit Domänenadminberechtigungen an

infor

Copyright © 2025. Infor. All Rights Reserved. infor.com

18

Das kann man so machen, das ist dann aber...



Sicherheitsfeatures abschalten



SMB1 einschalten



Keine alten Betriebssysteme betreiben
(oder so wenig wie möglich)



Niemals alte OS nach außen; also mit
Internetverbindung



Altdatensysteme sind folglich
abzulehnen

Das sollte man unbedingt machen:

Server

Backup immer auf separate Hardware

IP Filterlisten nutzen

Versionierung auf Fileservern nutzen

NTLMv1 und NTLMv2 abschalten

Separate Accounts für Administrative Tätigkeiten

JumpHosts für Administrative Tätigkeiten

Das sollte man unbedingt machen:

Clients

Office Makros deaktivieren

Scriptsprachen (JS/VBS) kontrollieren

Application Whitelisting

Separate Adminaccounts

Lokale Adminrechte minimieren

Lokale Adminpasswörter komplex und different



Copyright © 2025. Infor. All Rights Reserved. infor.com

21

Alles, was ein Bein nach außen hat, muss noch aktueller sein

Firewalls

Router

Exchange Server

VPN Gateways

Webserver



Copyright © 2025. Infor. All Rights Reserved. infor.com

22

Lessons learned aus Feuerwehr- einsätzen

Was tun gegen Ransomware?

Sei vorbereitet

- Notfallpläne erarbeiten

Habe Plattenplatz

- DEDUP funktioniert nicht mehr, wenn viele „neue“ Dateien durch Verschlüsselung hinzu kommen.
- Kopieren des kompromittierten Status quo notwendig
 - Beweissicherung
 - mögliche Quelle zum Datarestore

Restore üben

- Restore von vielen Maschinen ist erheblich langsamer!

Kommunikation kann schwierig werden

- Übliche Kommunikationskanäle müssen ggf. abgeschaltet werden



Copyright © 2025. Infor. All Rights Reserved. infor.com

23

Ansprechpartner

Christoph Marschibois

Christoph.Marschibois@infor.com

+49 211 8823 6741

+49 172 7481 586

Timo Haag

Timo.Haag@infor.com

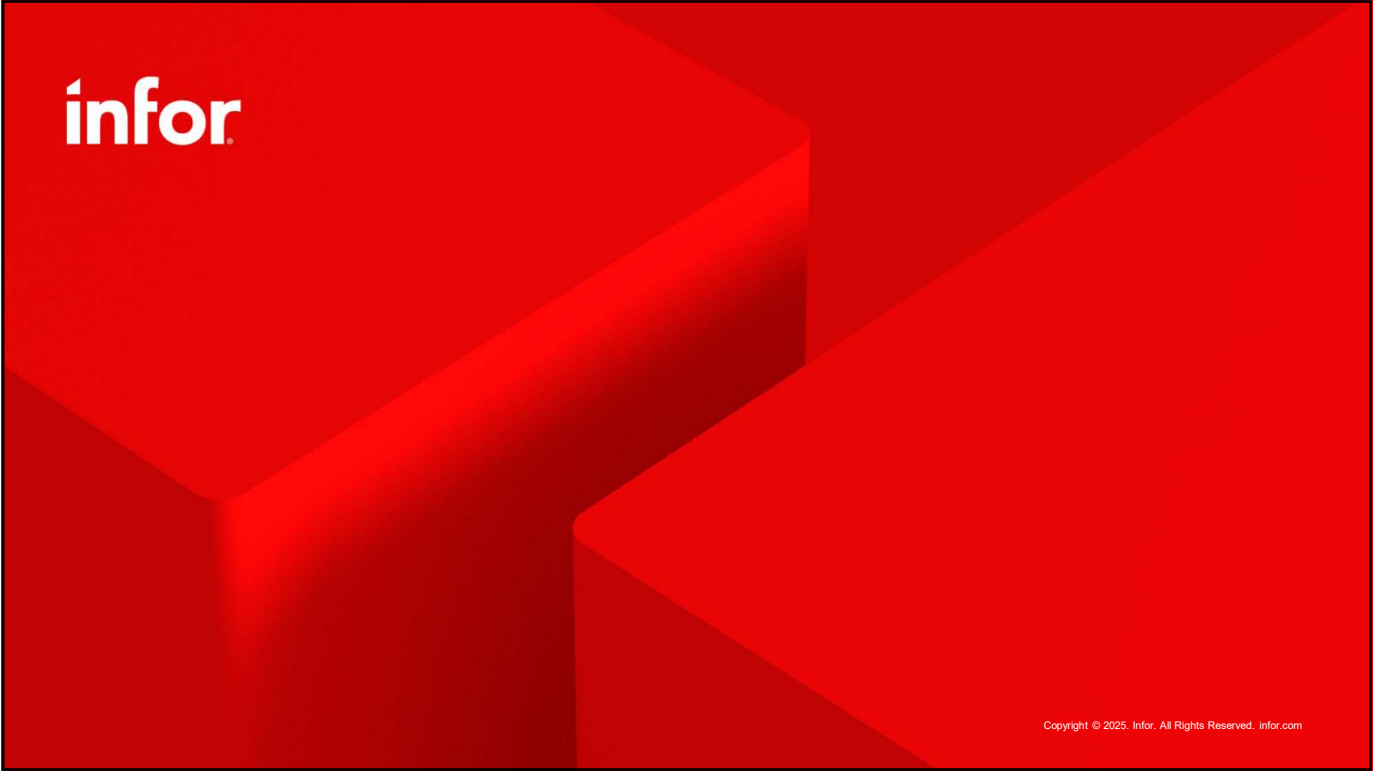
+49 211 8823 6910

+49 173 6681 748



Copyright © 2025. Infor. All Rights Reserved. infor.com

24

The image features a vibrant red background with abstract, three-dimensional geometric shapes that create a sense of depth and movement. The shapes are composed of various planes and angles, some of which are highlighted with a lighter red gradient, giving them a 3D appearance. In the top-left corner, the word "infor" is written in a clean, white, sans-serif font. In the bottom-right corner, there is a small, white copyright notice.

infor

Copyright © 2025. Infor. All Rights Reserved. [infor.com](https://www.infor.com)