$ecurity can‘t be bought!

marides, 28/12/2019

What are the
Security Requirements?

What is the Threat?

LIMITED RESSOURCES

A wall sometimes seems impossible to climb

PEOPLE

ORGANIZATION

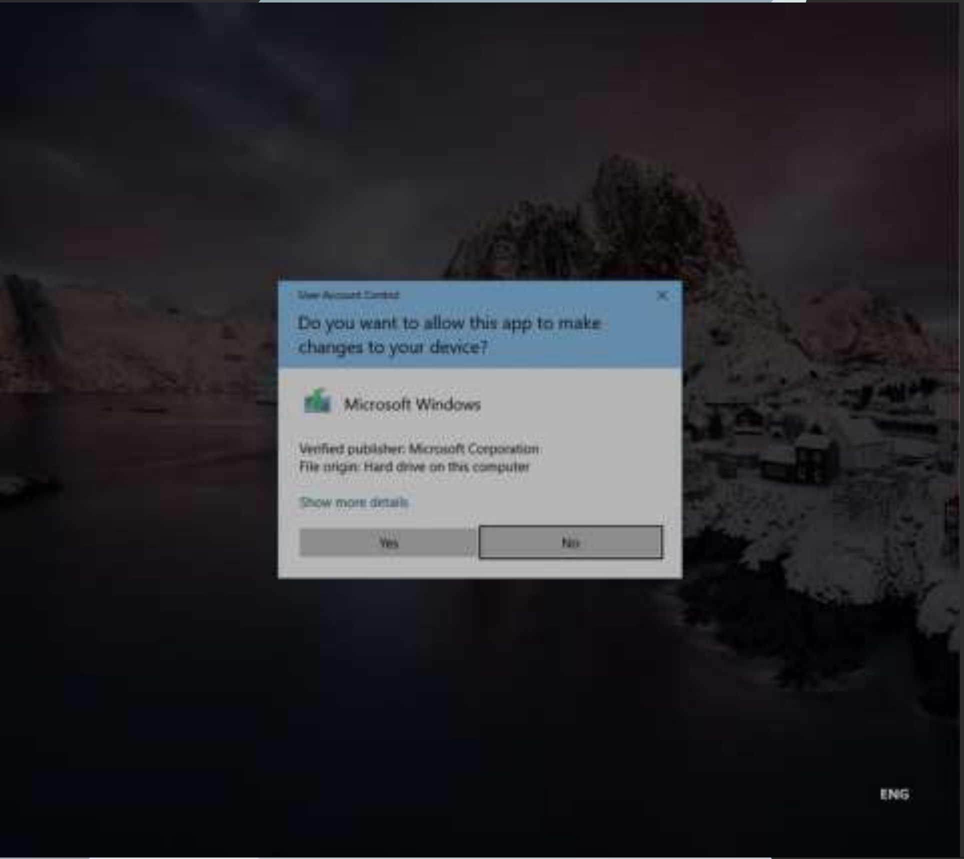
TECH

3 sections

01

PEOPLE

THE ONLY THING I HEAR IS :
MI MI MI MI
www.MOTOR-TALK.de

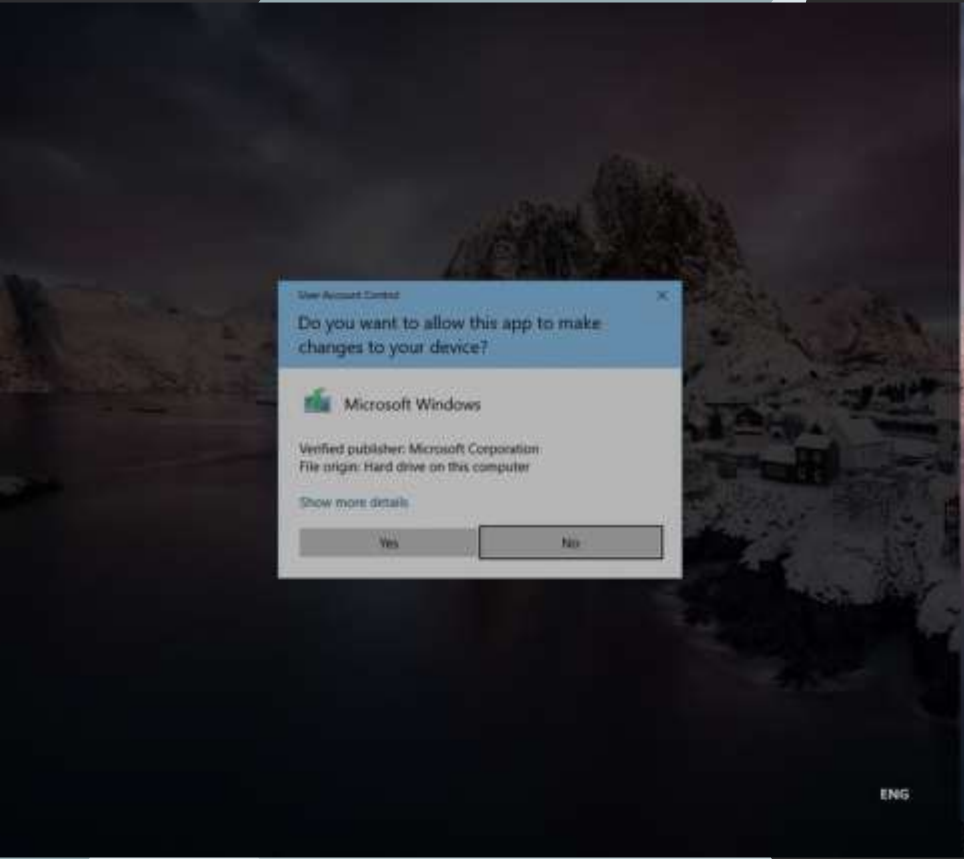


User Account Control

Do you want to allow this app to make changes to your device?

Microsoft Windows

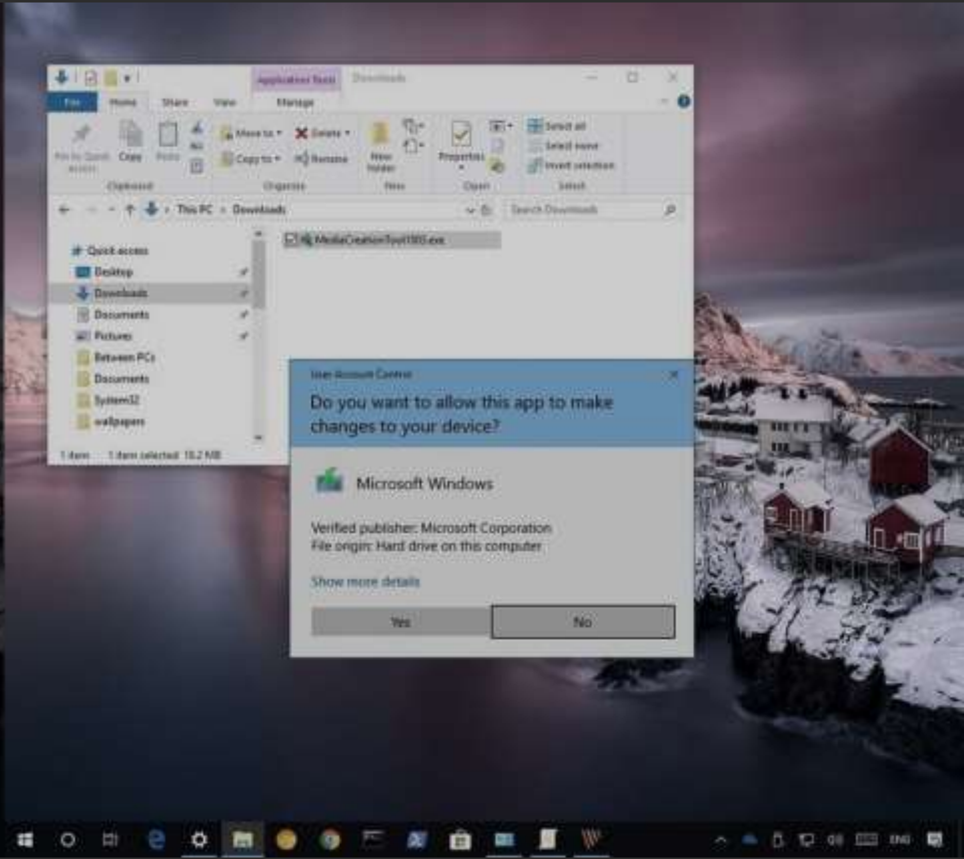
Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer


User Account Control

Do you want to allow this app to make changes to your device?

Microsoft Windows

Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer


User Account Control

Do you want to allow this app to make changes to your device?

Microsoft Windows

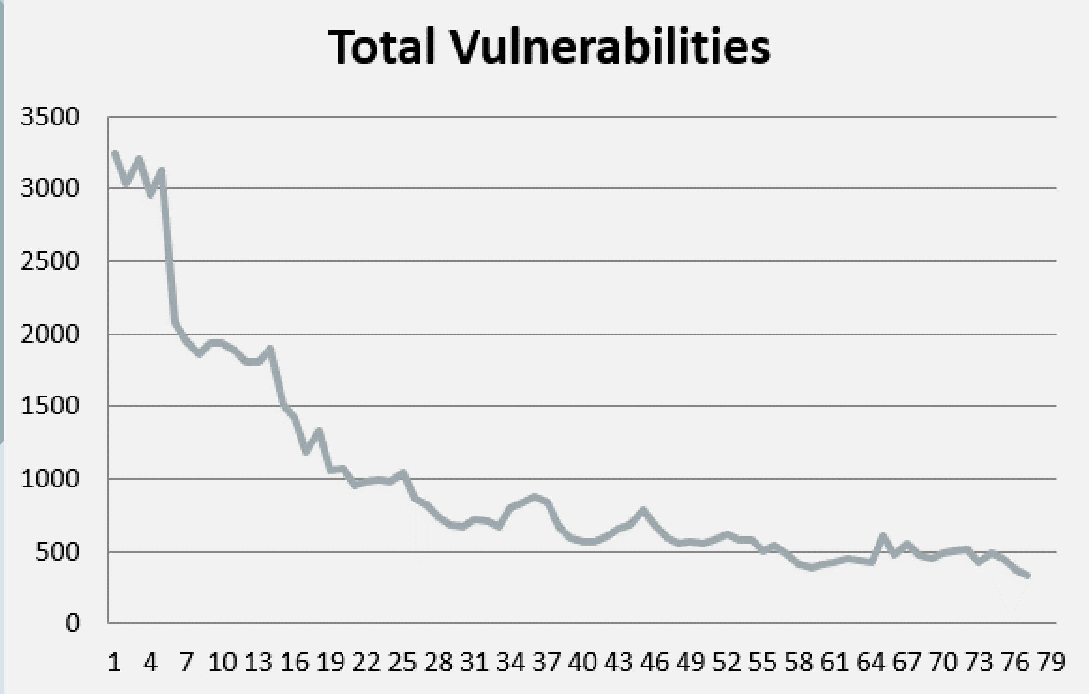
Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer

02

ORGANIZATION

Statistics

Vulnerabilities,
Spam,. . .


Total Vulnerabilities
3500
3000
2500
2000
1500
1000
500
0
1
4
7
10
13
16
19
22
25
28
31
34
37
40
43
46
49
52
55
58
61
64
67
70
73
76
79

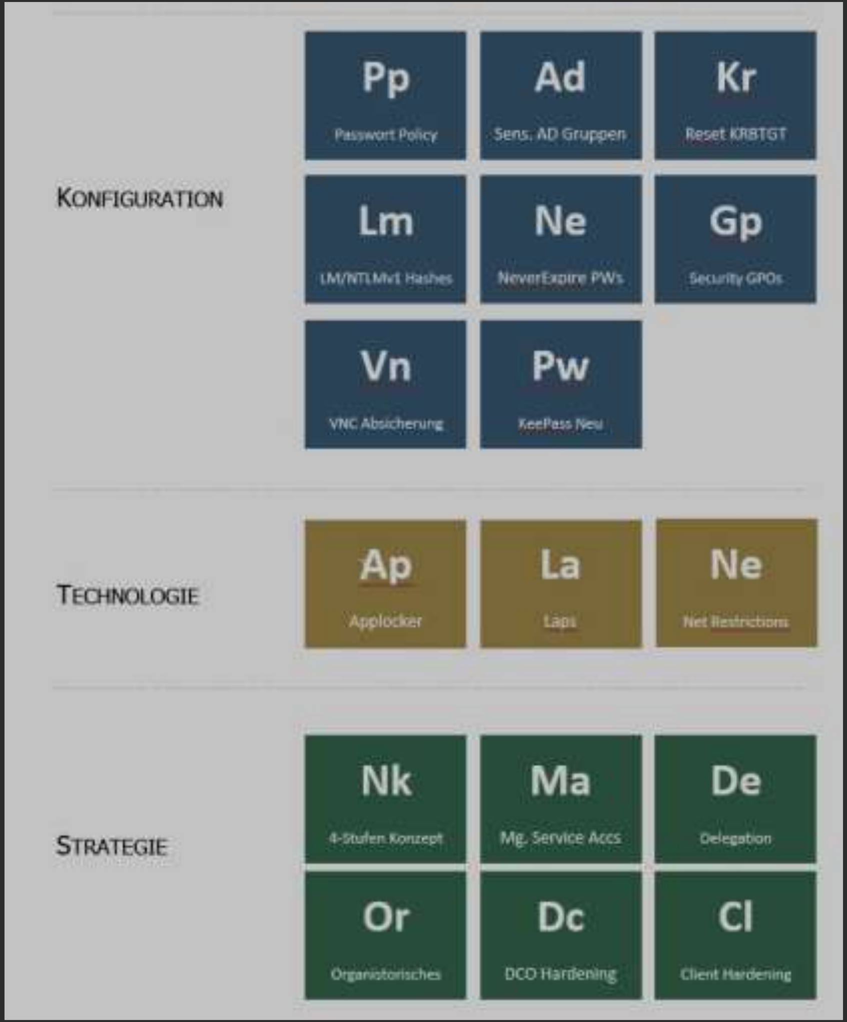
Statistics

Vulnerabilities, Spam,. . .

Brick Programms

Have a goal and end, focus on specific topics

Organization



Konfiguration

Pp Passwort Policy	Ad Sens. AD Gruppen	Kr Reset KRBTGT
Lm LM/NTLMv1 Hashes	Ne NeverExpire PWs	Gp Security GPOs
Vn VNC Absicherung	Pw KeePass Neu	

Technologie

Ap Applocker	La Laps	Ne Net Restrictions

Strategie

Nk 4-Stufen Konzept	Ma Mg. Service Accs	De Delegation
Or Organistorisches	Dc DCO Hardening	Cl Client Hardening

Statistics

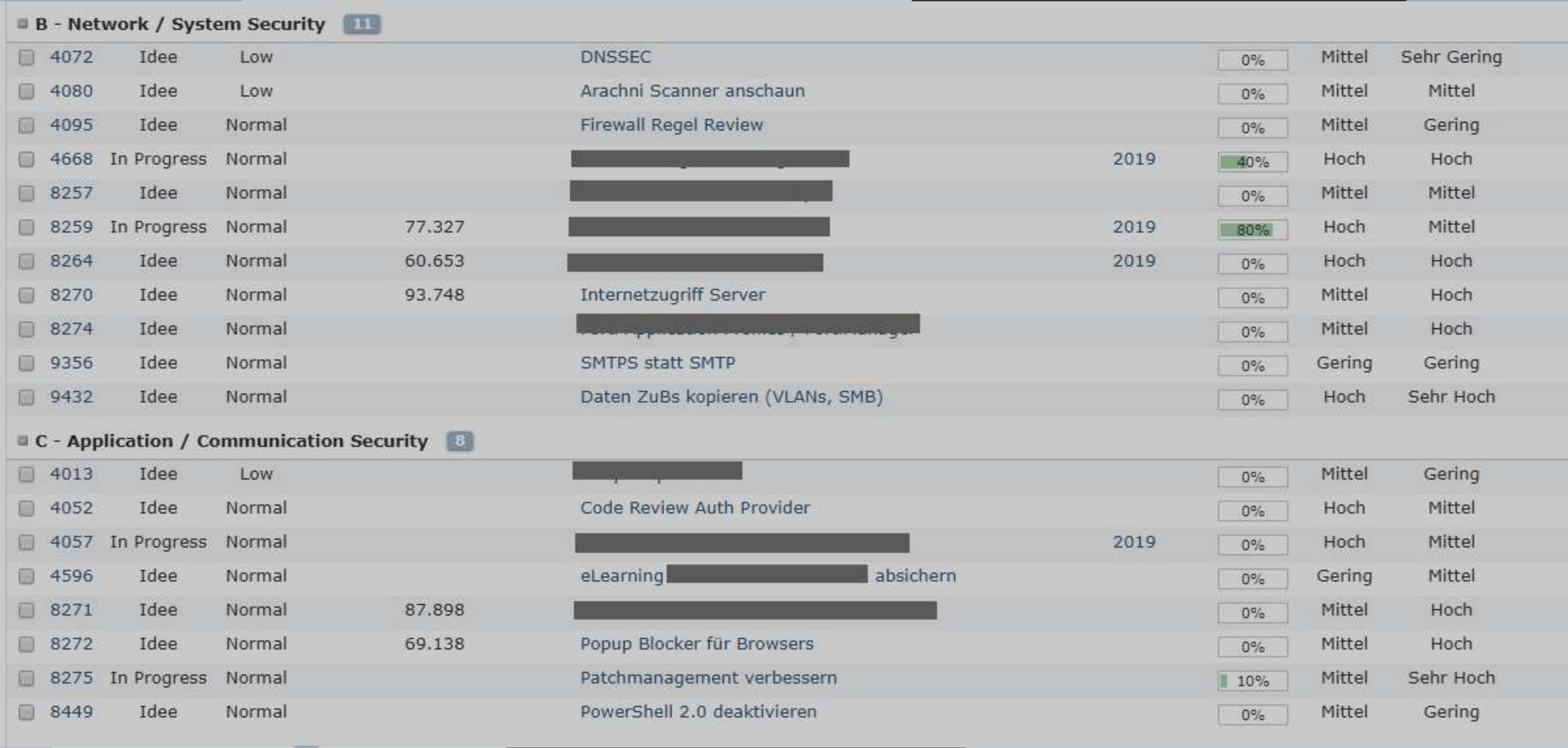
Vulnerabilities, Spam,…

Brick Programms

Have a goal and end, focus on specific topics

Idea repository

e.g.
Redmine Tracker



▪ B - Network / System Security 11

□	4072	Idee	Low		DNSSEC		0%	Mittel	Sehr Gering
□	4080	Idee	Low		Arachni Scanner anschaun		0%	Mittel	Mittel
□	4095	Idee	Normal		Firewall Regel Review		0%	Mittel	Gering
□	4668	In Progress	Normal		[redacted]	2019	40%	Hoch	Hoch
□	8257	Idee	Normal		[redacted]		0%	Mittel	Mittel
□	8259	In Progress	Normal	77.327	[redacted]	2019	80%	Hoch	Mittel
□	8264	Idee	Normal	60.653	[redacted]	2019	0%	Hoch	Hoch
□	8270	Idee	Normal	93.748	Internetzugriff Server		0%	Mittel	Hoch
□	8274	Idee	Normal		[redacted]		0%	Mittel	Hoch
□	9356	Idee	Normal		SMTPS statt SMTP		0%	Gering	Gering
□	9432	Idee	Normal		Daten ZuBs kopieren (VLANs, SMB)		0%	Hoch	Sehr Hoch

▪ C - Application / Communication Security 8

□	4013	Idee	Low		[redacted]		0%	Mittel	Gering
□	4052	Idee	Normal		Code Review Auth Provider		0%	Hoch	Mittel
□	4057	In Progress	Normal		[redacted]	2019	0%	Hoch	Mittel
□	4596	Idee	Normal		eLearning [redacted] absichern		0%	Gering	Mittel
□	8271	Idee	Normal	87.898	[redacted]		0%	Mittel	Hoch
□	8272	Idee	Normal	69.138	Popup Blocker für Browsers		0%	Mittel	Hoch
□	8275	In Progress	Normal		Patchmanagement verbessern		10%	Mittel	Sehr Hoch
□	8449	Idee	Normal		PowerShell 2.0 deaktivieren		0%	Mittel	Gering

Statistics

Vulnerabilities,
Spam,…

Brick Programms

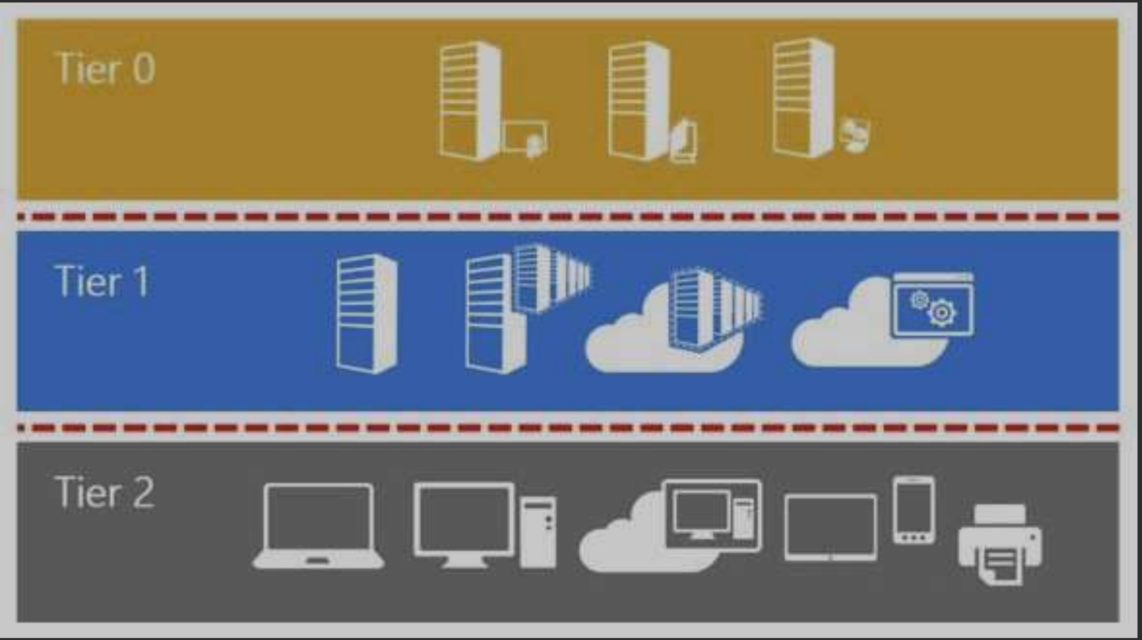
Have a goal and
end, focus on
specific topics

Idea repository

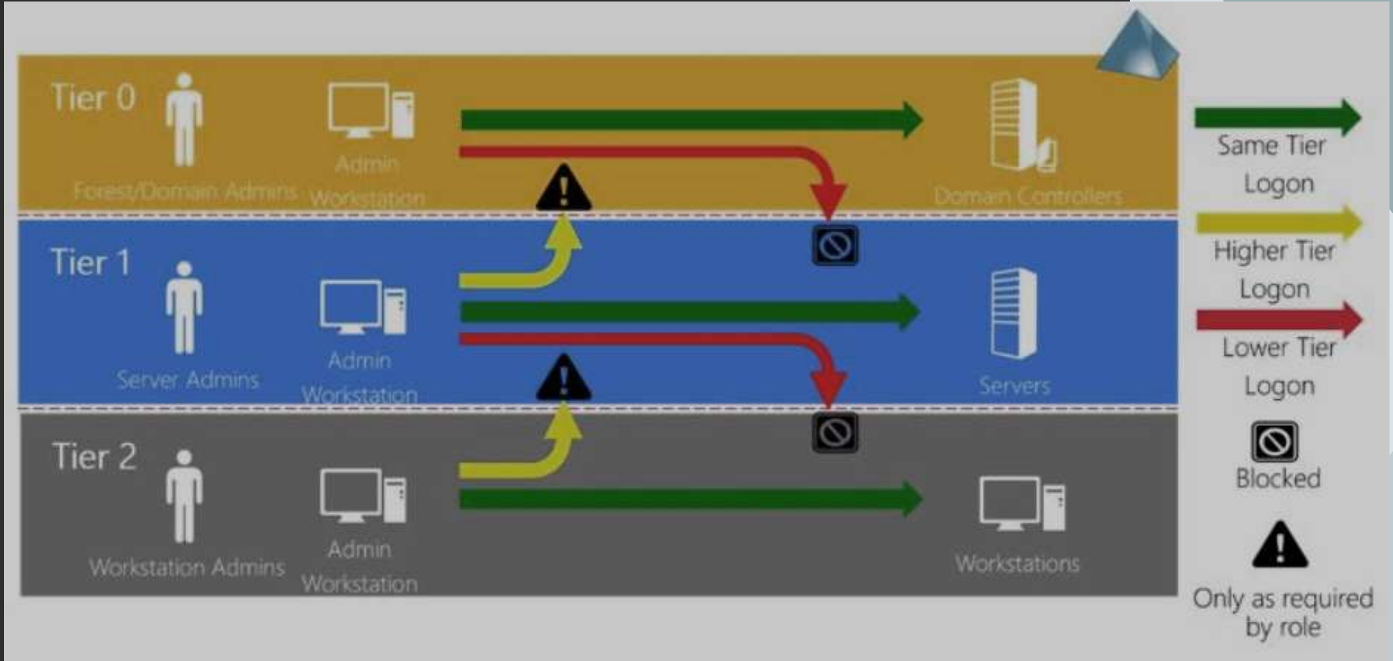
e.g.
Redmine Tracker

03

TECH



Core principle



Core principle

Quick Wins

- Use delegation (Account Operators)
- PowerShell Constrained Language Mode
- Reduce Membership in high-value groups
- Protected Users group
- Password manager
- FGPP (Fine Grained Password Policy)
- Passwords in Group Policy Preferences (GPPs)

„trackable“ Quick Wins

- Internal SSL Certificate Checker
- New user added to high-value group
- Domain Admin Logon
- Passwords in AD description
- New local admin on client/server

- SMB Versions (Encryption)
- No internet for servers
- Reduce Java / Flash
- Database Connection encryption
- Restrict Logon types

a little bit more time needed…

Deny logon…

	USERS	ADMINS	SERVICE ACCOUNTS
… through RDP	✗	✓	✗
… locally	✓	✓	✗
… as a service	✗	✗	✓
… as a batch job	✗	✗	✓
… from the network	On Computer object level (RPC, SMB…)		

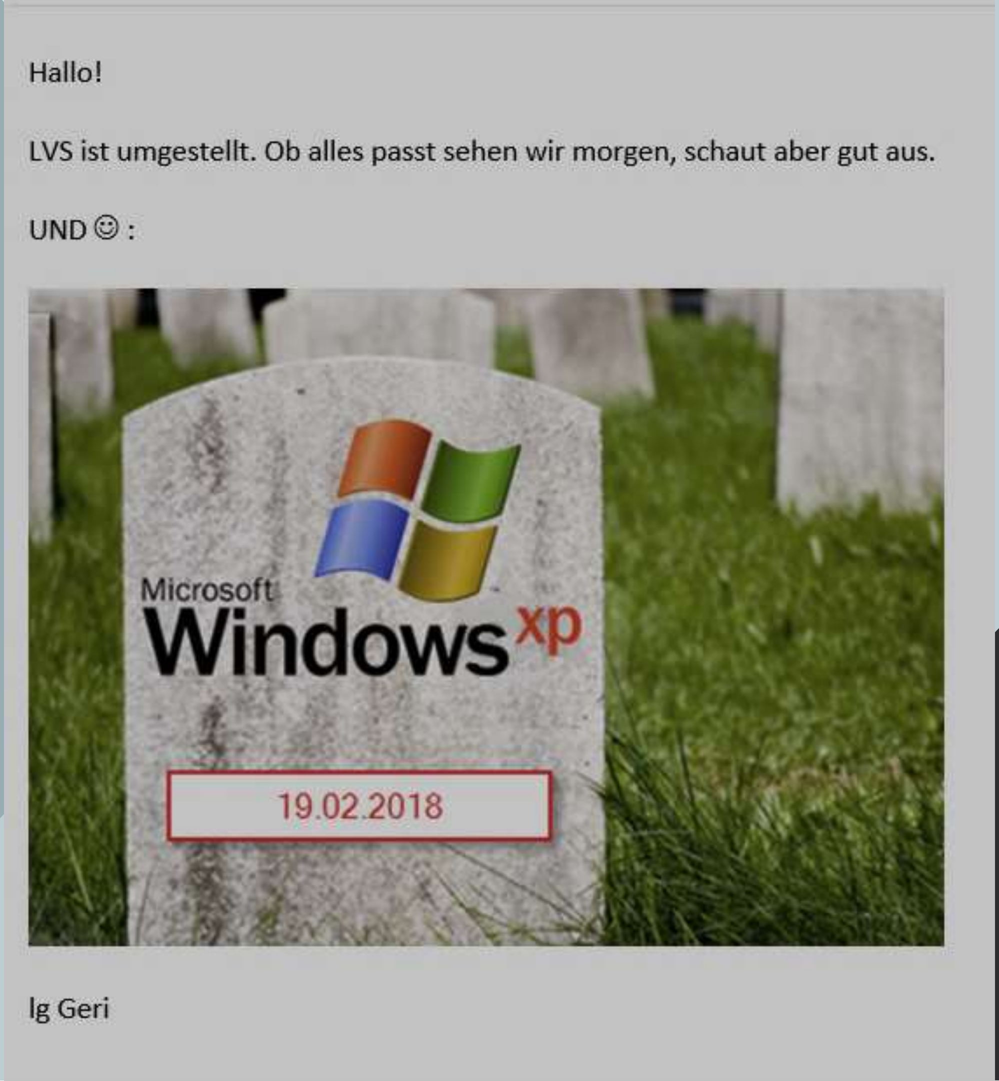
A little bit more time needed…

- SMB Versions (Encryption)
- No internet for servers
- Reduce Java / Flash
- Database Connection encryption
- Restrict Logon types
- gMSA or restrictions (Service accounts)
- LAPS
- SmartCard Logon for Admins (enforced)

A little bit more time needed…

- SMB Versions (Encryption)
- No internet for servers
- Reduce Java / Flash
- Database Connection encryption
- Restrict Logon types
- gMSA or restrictions (Service accounts)
- LAPS
- SmartCard Logon for Admins (enforced)

The right thing?

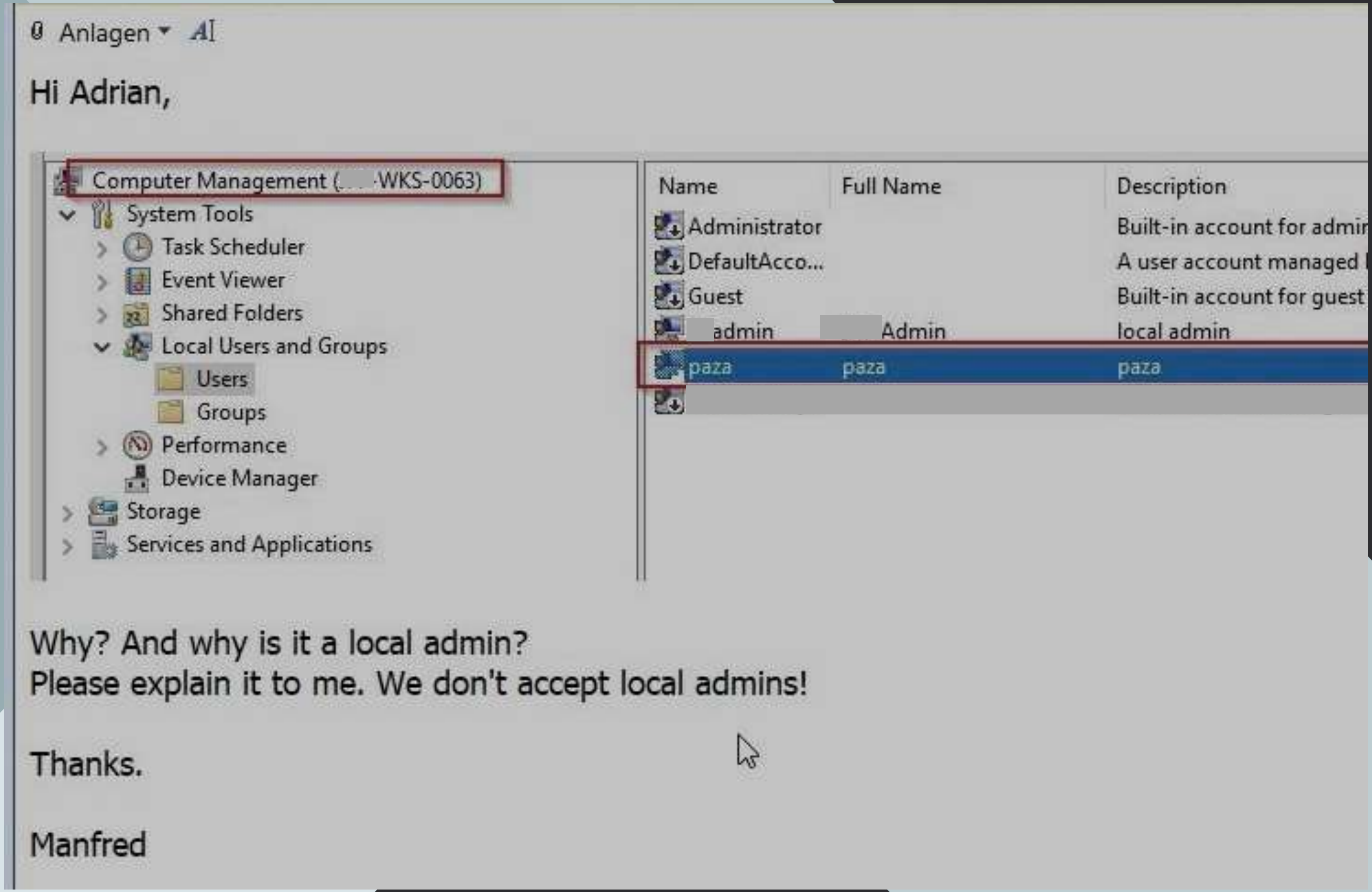


Hallo!

LVS ist umgestellt. Ob alles passt sehen wir morgen, schaut aber gut aus.

UND ☺ :

lg Geri



Hi Adrian,

Name	Full Name	Description
Administrator		Built-in account for admi
DefaultAcco...		A user account managed
Guest		Built-in account for guest
[redacted]admin	[redacted] Admin	local admin
paza	paza	paza
[redacted]		

Why? And why is it a local admin?
Please explain it to me. We don't accept local admins!

Thanks.

Manfred

PEOPLE → Stop Complaining,
Start Listening.

ORGANIZATION → Make it visible!

TECH → Prioritization is Key!

Thanks!

marides@L3L3.org
Telegram: MaridesRosa

Credits

- Mitigating Pass-the-Hash and Other Credential Theft, version 2: https://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf
- Microsoft 3 Tier Model: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material
- Redmine Tracker: https://www.redmine.org/
- Alternative Methode zur Priorisierung von Sicherheitsmaßnahmen: https://bogner.sh/2019/04/alternative-methode-zur-priorisierung-von-informations-sicherheitsmasnahmen-german/
- Powershell Constrained Language Mode: https://www.windowspro.de/wolfgang-sommergut/constrained-language-mode-powershell-risiken-entschaerfen
- What could happen – Darknet Diaries: NotPetya (Podcast): https://darknetdiaries.com/episode/54/