

13 ERFOLGREICHE WEGE, DIE IT-INFRASTRUKTUR IHRES KUNDEN IN DIE ERDE ZU RAMMEN

(UND WIE MAN SIE VERMEIDET)



Cactus Bodyslam.

TEIL 1:

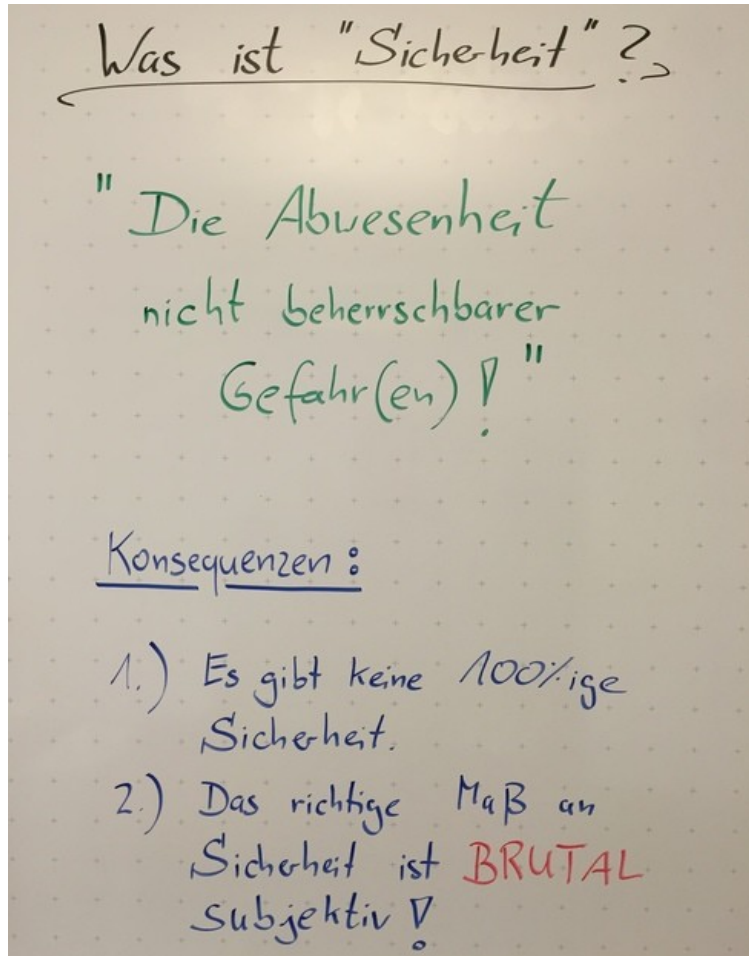
DIE GRUNDLAGE DES ERFOLGREICHEN SCHEITERNS

IT-Infrastruktur in die Erde rammen – Version 241109 – [Klassifizierung: intern] – Folie 3




**KÜMMERN SIE SICH
NICHT DARUM, WAS
“SICHERHEIT”
EIGENTLICH IST.**

BEGRIFFSDEFINITION: WAS IST SICHERHEIT?



- » Keine angemessene Sicherheit ohne Kenntnis der Anforderungen: Wer verlangt was von Ihnen in Sachen Sicherheit?
- » Informationssicherheit ist keine Frage der technischen Ausstattung, sondern ein Teamsport in verschiedenen Disziplinen.
- » Diplomatie ist gefragt: Sie müssen zuhören, argumentieren, akzeptieren, Kompromisse eingehen.
- » Sie sind Techniker, Sozialpädagoge (na ja... vielleicht eher Rechtsanwalt!) und Außenminister in einer Person.
- » Merke: Wenn Sie sich um (Informations-)Sicherheit kümmern wollen/sollen/müssen, arbeiten Sie vor allem mit Menschen.



Ihre Aufgabe:
Konsequent die Weichen
in Richtung Abgrund stellen!

TEIL 2:

TIPPS FÜR DIE

GRUNDLEGENDE

HERANGEHENSWEISE

A large, yellow, multi-pointed starburst shape with a black outline, centered on the slide. It contains two lines of bold, black, uppercase text.

**VERKAUFEN SIE IMMER
DAS, WAS SIE HABEN!**

**DER BAUHLADEN
MUSS LEER WERDEN!**

RUDIMENTÄRE CHECKLISTE: ANALYSE

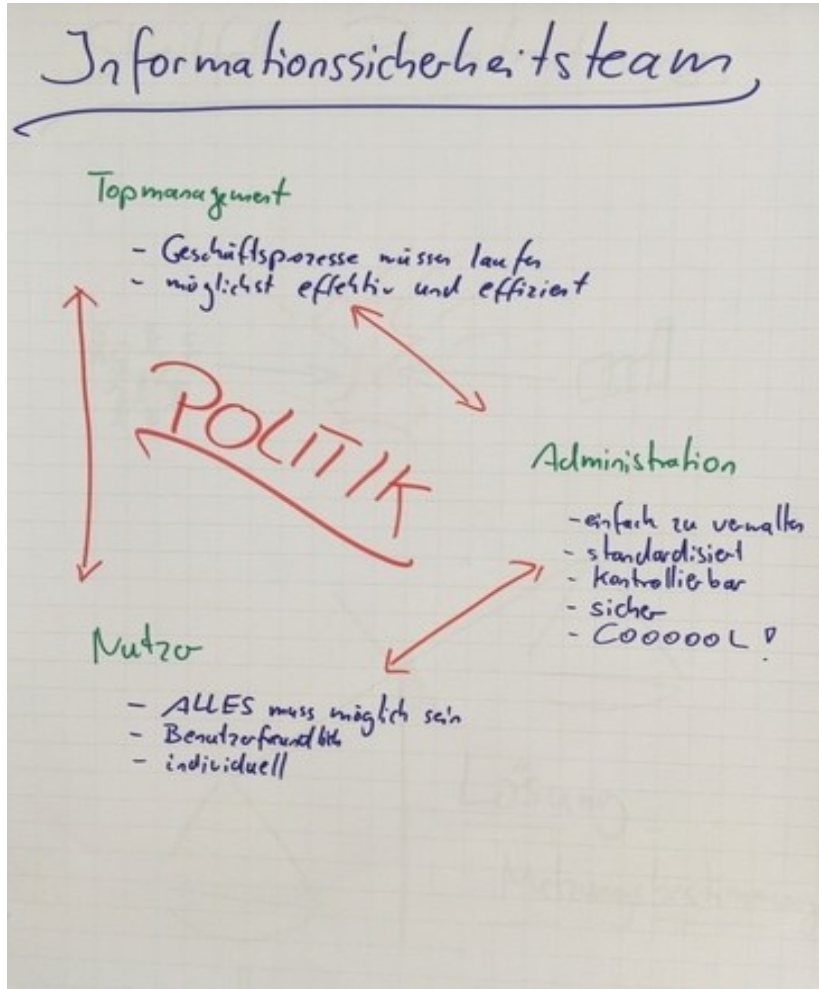
- » Ermitteln Sie, wer Anforderungen an die Sicherheit Ihres Kunden stellt:
 - » Gesetzliche Anforderungen?
 - » Vertragliche Anforderungen (Kunden, Lieferanten, Verbände, ...)?
 - » Betriebliche Anforderungen (Prozesse, Mitarbeiter, Dienstleister, ...)?
- » Ermitteln Sie, welche Anforderung die einzelnen Parteien stellen:
 - » Verfügbarkeit, Vertraulichkeit, Integrität?
 - » Wird die Umsetzung konkreter Normen/Standards/Richtlinien gefordert?



**BEGREIFEN SIE
SICHERHEIT ALS REIN
TECHNISCHES PROBLEM.**

**ES GILT:
EIN PROBLEM, EIN PRODUKT,
EINE LÖSUNG!**

RUDIMENTÄRE CHECKLISTE: ORGANISATION



» Management, Anwender und Techniker sollten sich in einer offenen Runde austauschen.

- » Welche Anforderungen gibt es?
- » Wie können wir sie gemeinsam erfüllen, ohne die Sicherheit zu gefährden?
- » Welche Probleme gibt es?
- » Wo soll die IT in 5 Jahren angekommen sein?



A large, yellow, multi-pointed starburst shape with a black outline, centered on the slide. It contains two lines of bold, black, uppercase text.


**AUS DEN AUGEN,
AUS DEM SINN!**

**MERKE: DER NÄCHSTE KUNDE
WARTET SCHON AUF IHRE
FACHMÄNNISCHE
UNTERSTÜTZUNG!**

MANGED SERVICES

- » Verkaufen Sie kein Produkt.
- » Betreuen Sie Ihre Kunden.





Ihre Aufgabe:
Draufhalten und Gas geben!

TEIL 3:

TIPPS FÜR IHRE TECHNIES



**SIE SIND
TECHNIKER.**

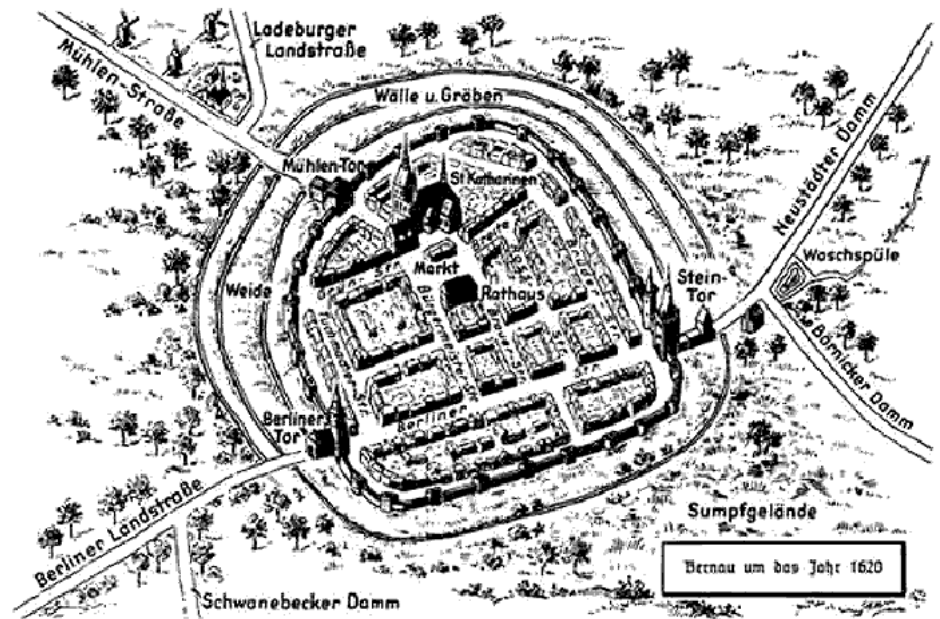
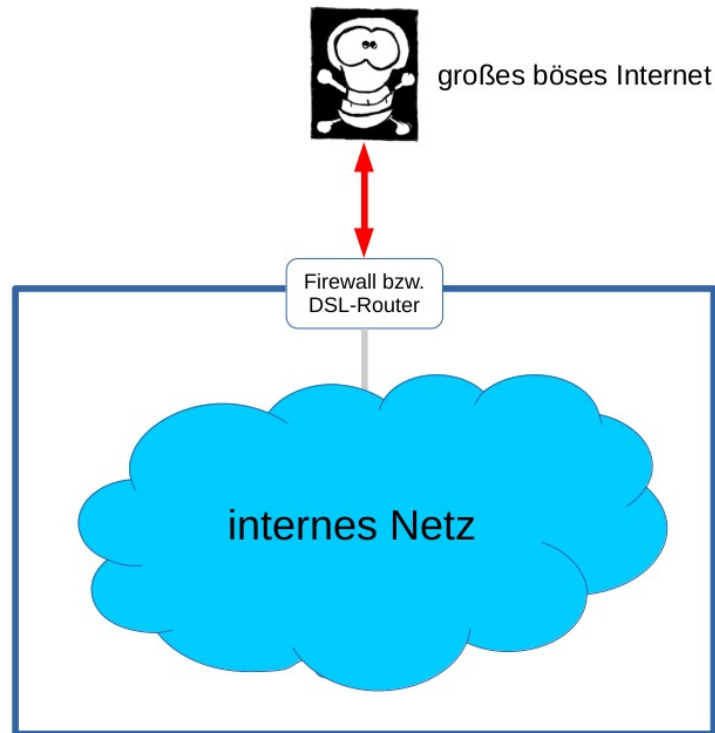
**MACHEN SIE DEN
SERVERSCHRANK ZU.
VON INNEN.**

A large, yellow, multi-pointed starburst shape with a black outline, centered on the slide. It contains two lines of bold, black, uppercase text.

**STRUKTURIEREN SIE
DAS NETZ IHRES KUNDEN
MÖGLICHST FLACH!**

SEGMENTIERUNG IST BÖSE!

SO SEHEN DIE MEISTEN NETZE AUS. WILLKOMMEN IM MITTELALTER!



RUDIMENTÄRE CHECKLISTE SEGMENTIERUNG

- » Sind Kriterien festgelegt, anhand derer das Netz in Zonen unterteilt wird, wie z. B.
 - » Vertrauenswürdigkeit der IT-Systeme
 - » Robustheit der IT-Systeme
 - » Einsatzzweck der IT-Systeme
 - » ...
- » Sind die Zonen voneinander abgeschottet?
 - » Kommunikationsmatrix?
 - » ACLs zwischen Netzen?
 - » Client Separation (Private VLANs) aktiviert?
 - » Remote-Access gem. Least Privileges organisiert?



A large, yellow, multi-pointed starburst shape with a black outline, centered on the slide. It contains two lines of bold, black, uppercase text.


**ORGANISIEREN SIE DIE
ADMINISTRATION
MÖGLICHST FLACH.**

**JEDER ADMIN
MUSS ALLES TUN DÜRFEN.
EGAL WO. EGAL WANN.**

CHECKLISTE ADMINPRIVILEGIEN

- » Arbeitet jemand als Domain-Admin?
 - » Packen Sie ALLE Domain-Admins in den Giftschrank für absolute Notfälle.
- » Administration in verschiedene Zonen unterteilt?
 - » Vertrauenswürdigkeit der dortigen IT-Systeme
 - » Einsatzzweck der dortigen IT-Systeme
 - » Kritikalität der dortigen IT-Systeme
 - » Empfehlung: 4 Stufen: Backend-Server, interne Server, DMZ, Clients
- » Schutz der administrativen Zonen vorhanden
 - » Least Privileges?
 - » Zwei-Augen-Prinzip?
 - » Accounting?
- » Mehr-Faktor-Authentifizierung für Admins!





**VERSTEHEN SIE
BACKUP UND RECOVERY
ALS EINFACHES,
LÄNGST GELÖSTES UND
REIN TECHNISCHES
PROBLEM.**

RUDIMENTÄRE CHECKLISTE DATENSICHERUNG

» Speicherorte

- » Erfasst bzw. organisatorisch geregelt?
- » Strukturiert verwaltet (technische Mindeststandards, Orga)?
- » MTA und MTD definiert?

» Technik

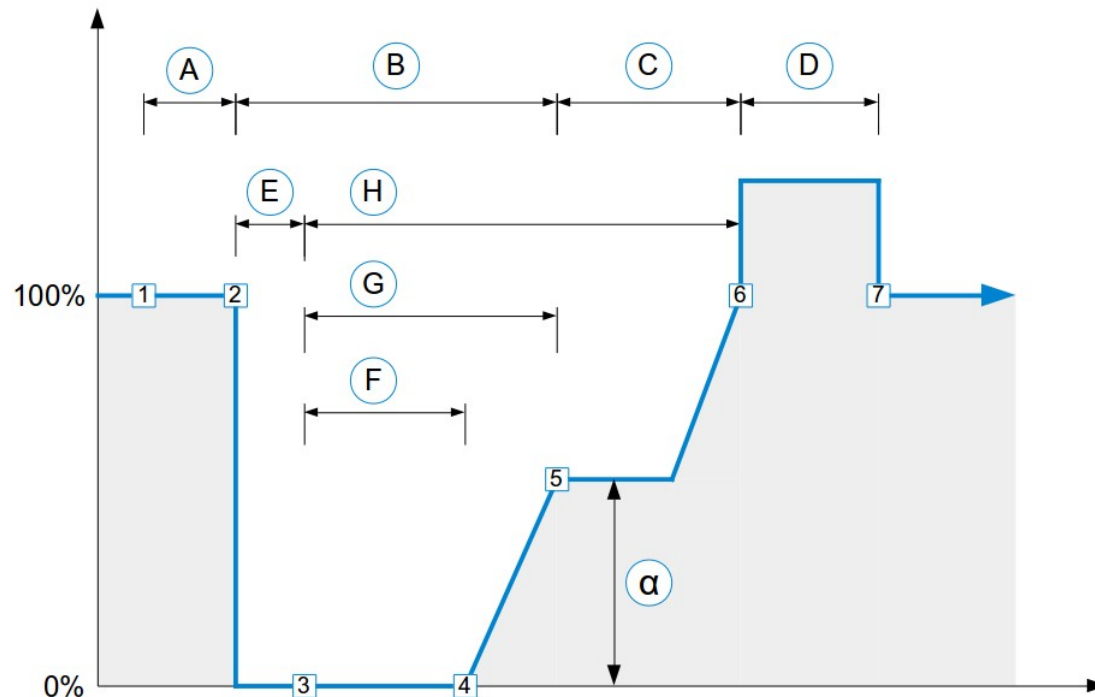
- » Mehr-Generationen-Prinzip?
- » Redundante Speicherung?
- » Verteilte Standorte?
- » Backup-Infrastruktur möglichst umfassend gekapselt?

» Orga

- » Verantwortliche definiert?
- » Wiederherstellungsplan (Kochrezept) vorhanden?
- » Wiederherstellungsplan wird zyklisch getestet?



BACKUP UND RECOVERY: MTD UND MTA



» Ereignisse


- » 1 Letzte Datensicherung
- » 2 Ausfall des Systems
- » 3 Entdeckung des Ausfalls
- » 4 Start der Wiederherstellung
- » 5 Anlaufen des Notbetriebsniveaus
- » 6 Vollständige Wiederherstellung
- » 7 Aufnahme des Regelbetriebs

» Zeiträume:

- » A Zeitraum ohne Datensicherung
(Maximal tolerierbarer Datenverlust MTD)
- » B Ausfallzeit
(Maximal tolerierbare Ausfallzeit MTA)
- » C Dauer des Notbetriebs
- » D Nacharbeit
- » E Zeit bis zur Entdeckung des Ausfalls
- » F Reaktionszeit
- » G Zeit bis Aufnahme des Notbetriebs
- » H Zeit bis zur Wiederherstellung

» Betriebszustände

- » a) Notbetriebsniveau



Mit Höchstgeschwindigkeit
die Kollision genießen!

TEIL 3:

WEITERE COOLE TECHNIK-TIPPS

A large, yellow, multi-pointed starburst shape with a black outline, centered on the slide. It contains two lines of bold, black, uppercase text.

**HALTEN SIE PASSWÖRTERN
DIE TREUE.**

**MFA IST EINE AUSGEBURT
DER HÖLLE.**

A large, yellow, multi-pointed starburst shape with a black outline, centered on the slide. It contains two lines of bold, black, uppercase text.

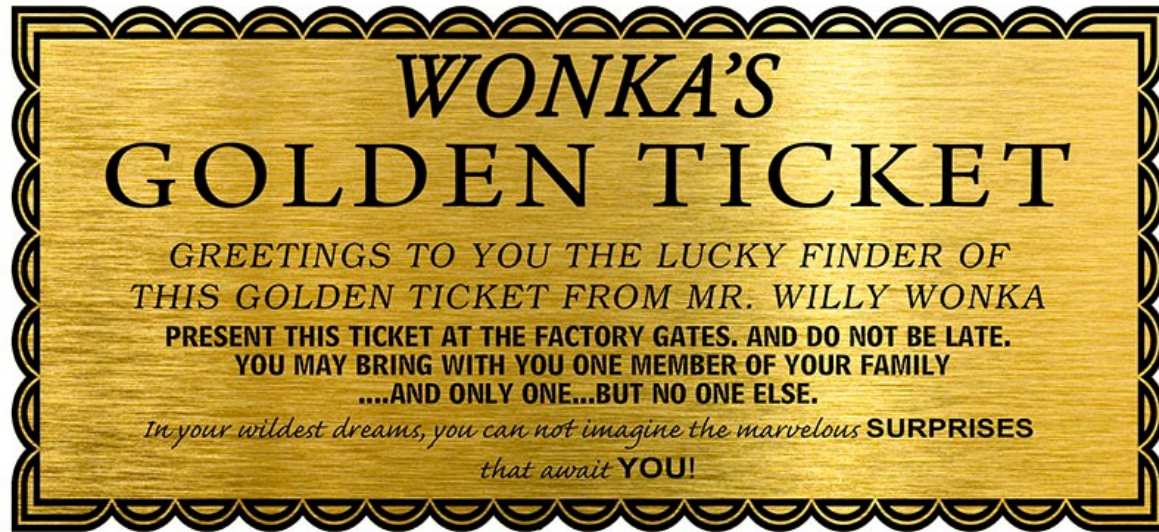
**BETREIBEN SIE
MS ACTIVE-DIRECTORY
OUT-OF-THE-BOX.**

**SIE SCHLIEßEN JA AUCH
IHR FAHRRAD NICHT AB.**

MICROSOFT ACTIVE DIRECTORY (AD)

- » Zentrale Verwaltung von Konten und Zugriffsrechten.
- » Zentrale Authentifizierung und Autorisierung über das Kerberos-Protokoll.
- » Grundlegende Prinzipien von Kerberos:
 - » Verschiedene Instanzen stellen Tickets aus. Tickets autorisieren Aktionen.
 - » Tickets sind verschlüsselt. Sie werden von der prüfenden Instanz validiert, indem sie entschlüsselt werden.
- » Ein besonderes Ticket (das Ticket-Granting-Ticket – kurz: TGT) wird mit dem NTLM-Hash des AD-Accounts „krbtgt“ verschlüsselt.
- » Wenn der Angreifer den NTLM-Hash des Accounts „krbtgt“ besitzt, kann er sich im Namen des Kerberos-Systems beliebige Tickets ausstellen.

KERNBOHRUNG FÜR MS ACTIVE-DIRECTORY

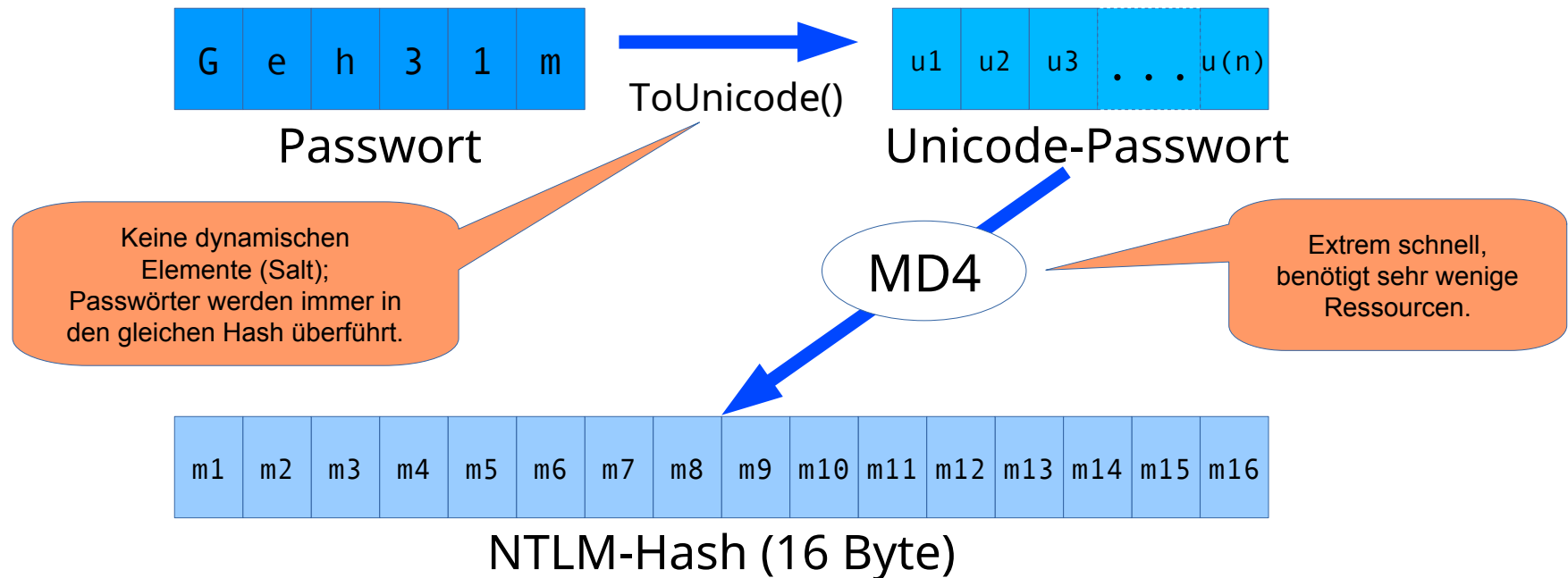


» Nähere Informationen:

- » [https://www.andreafortuna.org/2020/05/05/\(...\)](https://www.andreafortuna.org/2020/05/05/(...))
- » [https://www.blackhat.com/docs/us-14/\(...\)](https://www.blackhat.com/docs/us-14/(...))

THE GOOD(?) OLD (!) NTLM-HASH...

- » Passwörter werden von MS Windows nicht als Klartext gespeichert, sondern in gehashter Form. Das Standard-Format der gehashten Windows-Passwörter lautet NTLM und wurde mit Windows NT 4.0 SP3 (!) eingeführt.
- » So arbeitet NTLM:



NTLM IST HOCHGRADIG VERWUNDBAR

- » **Problem: keine variablen Anteile; gleiche Passwörter werden immer in den gleichen Hash umgewandelt**
 - » Ermöglicht vorberechnete Wörterbücher „Hash → Passwort“.
 - » Diese sind verfügbar (als Rainbow-Tables).
 - » Geklaute Hashes können in Wörterbüchern nachgeschlagen werden; bekannte Passwörter fallen innerhalb von Sekunden(-bruchteilen).
- » **Problem: MD4 benötigt extrem wenig Ressourcen**
 - » Brute-Force-Angriffe (das stupide Ausprobieren aller möglichen Passwörter) sind für Passwörterlängen möglich, die in der Praxis eingesetzt werden und allgemein als „sicher“ wahrgenommen werden.
 - » Komplexe Rateangriffe gegen längere Passwörter können einfach durchgeführt werden.
- » **Mit Equipment für weit unter € 15.000,- fallen...**
 - » ...gebräuchliche Passwörter in wenigen Sekunden bis Minuten
 - » ...beliebig komplexe Passwörter mit 8 Zeichen Länge innerhalb von 2,5 Stunden
 - » ...beliebig komplexe Passwörter mit 9 Zeichen Länge innerhalb von 8 Tagen
 - » ...eine ganze Reihe semi-komplexer Passwörter mit (weit) mehr als 9 Zeichen.

DIE FOLGEN IN DER PRAXIS? VERHEEREND!

- » Wenn der Angreifer im Besitz eines NTLM-Hashes gelangt, erhält er in aller Regel auch das dazugehörige Passwort im Klartext.
- » Die Schwächen von NTLM sind seit Jahren bekannt.
- » NTLM wird aber aus Kompatibilitätsgründen noch immer standardmäßig im AD verwendet...



NTLM-HASHES KLAUEN AUF EINEM AD-CLIENT

- » Rahmenbedingungen:
 - » Der Prozess „lsass.exe“ (LSASS = Local Security Authority Subsystem Service) authentifiziert die einloggenden User.
 - » LSASS (aber auch andere Prozesse) speichert standardmäßig die NTLM-Hashes der Passwörter von erfolgreich eingeloggten Usern im RAM zwischen.
 - » Programme, die von einem Nutzer mit dem Privileg „Debug programs“ (SeDebugPrivilege) gestartet wurden können beliebige Prozesse debuggen und u. a. auch Speicherabbilder dieser Prozesse erzeugen.
 - » Folge: User mit dem Privileg gelangen an NTLM-Hashes.
- » Das Tool Mimikatz z. B. erledigt die Arbeit.
 - » <https://github.com/gentilkiwi/mimikatz>
- » Angriff ist erfolgreich, wenn...
 - » ...der User, der den Angriff startet das Privileg „Debug programs“ besitzt
 - » ...der lokale Anti-Virus ein verwendete Tool nicht erkennt
 - » ...der Credential Guard nicht anwesend ist (der ist nur bei Windows 10 Enterprise ab Version version 20H1 vorhanden) und
 - » ...der Nutzer nicht Mitglied in der AD-Gruppe „Protected Users“ ist.

GEGENMAßNAHMEN (EINSTIEG)

- » Lernen Sie AD kennen.
 - » Informieren Sie sich über die Schwachstellen von AD.
 - » Sogar Microsoft bietet hier gute Informationen (z. B. [hier](#)).
 - » Kümmern Sie sich um Service Accounts (Infos z. B. [hier](#)).
- » Verwenden Sie Tools, die die Konfiguration eines AD prüfen bzw. härten, z. B.
 - » PingCastle (<https://www.pingcastle.com>)
 - » BloodHound (<https://specterops.io/bloodhound-overview/>) oder
 - » Directory Services Protector (<https://www.semperis.com/active-directory-security/>)
- » Bieten Sie diese Dienste Ihren Kunden als Abo an.

A large, yellow, multi-pointed starburst shape with a black outline, centered on the slide. It contains two lines of bold, black, uppercase text.

**BEWAREN SIE ALLE
BETEILIGTEN VOR ZU VIEL
WISSEN.**

**SORGEN SIE DAFÜR,
DASS NIEMAND LOGS
LESEN KANN!**

GEGENMAßNAHMEN (EINSTIEG)

- » Etablieren Sie ein möglichst zentralisiertes Logging.
 - » Aufbau von einem (oder von einigen wenigen) Logserver(n).
 - » Bringen Sie Server, aktive Netzwerkkomponenten (Switches, Router, Firewalls, WLAN-Controller, ...) und ggf. auch (ausgewählte) Clients dazu, ihre Logmeldungen an diese(n) Server zu senden. Das geht i. d. R. mit den eingebauten Bordmitteln.
 - » Kapseln Sie Logserver vom Rest der IT-Infrastruktur möglichst umfassend.
- » Legen Sie fest, welche Meldungen wahrscheinlich wichtig sind.
 - » Logmeldungen mit sehr hoher Priorität.
 - » Meldungen vom Antivirus
 - » Meldungen vom Backup-System
 - » Meldungen über das Anlegen von Accounts
 - » Meldungen über das Erhöhen von Rechten
 - » ...
- » Lassen Sie sich beim Eintreffen von ausgewählten Meldungen aktiv benachrichtigen und schauen Sie in regelmäßigen Abständen in die Logs.
- » Keine Angst – dafür gibt es Software.



**SUCHEN SIE NIEMALS
NACH SCHWACHSTELLEN.**

GEGENMAßNAHMEN (EINSTIEG)

- » Bieten Sie ihren Kunden an, ihre Netzwerkkumgebung in regelmäßigen Abständen mit einem Security-Scanner zu überprüfen.
- » Die bekanntesten Allround-Scanner sind z. B.
 - » Nessus (<https://www.tenable.com/products/nessus>)
 - » Greenbone (<https://www.greenbone.net/>)
 - » ...
- » Behandeln Sie entdeckte Sicherheitslücken wie Sicherheitsvorfälle.
 - » Priorisierung
 - » Behebung
 - » Nachbereitung



**UPDATES IST FÜR
WEICHEIER.**

GEGENMAßNAHMEN (EINSTIEG)

- » Bieten Sie ihren Kunden an, ausgewählte Software auf dem aktuellen Stand zu halten, z. B.
 - » Software, die für den Betrieb der Kernprozesse benötigt wird.
 - » Software, die im Internet exponiert ist (DMZ).
 - » Software, die Content aus dem Internet verarbeitet (Browser, Mailclient, ...).
- » Legen Sie dabei fest:
 - » Welche Software wird aktualisiert?
 - » Welche Updates werden eingespielt (Feature/Security, Prio, ...)?
 - » Wann werden welche Updates eingespielt (Patchday, Emergency-Updates)?
 - » Wie werden die Updates im Vorfeld getestet?

ZUSATZMATERIAL

(KEINE ANGST VOR ISMS!)

WAS IST EIN ISMS?

» Ein Informationssicherheitsmanagementsystem (ISMS)...

- » ...ist eine Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern (anzupassen).
- » ...stellt sicher, dass Informationssicherheit nach dem Motto „So viel wie nötig, so wenig wie möglich“ implementiert und auf dem aktuellen Stand gehalten wird.
- » ...kann man als „Qualitätsmanagement für die Informationssicherheit“ bezeichnen.

» ACHTUNG!

- » Ein ISMS sollte so schlank wie möglich implementiert werden.
- » Es hat immer die Aufgabe, Informationssicherheit nach dem Motto „So wenig wie möglich und so viel wie nötig!“ zu implementieren.

EIGENSCHAFTEN UND ZIELE EINES ISMS (1)

- » Verankerung in der Organisation:
Die Verantwortlichkeiten und Befugnisse für den Informationssicherheitsprozess werden vom Topmanagement eindeutig und widerspruchsfrei zugewiesen. Insbesondere wird ein Mitarbeiter bestimmt, der umfassend verantwortlich für das Informationssicherheitsmanagementsystem ist (in der Regel Informationssicherheitsbeauftragter oder kurz ISB).
- » Verbindliche Ziele:
Die durch den Informationssicherheitsprozess zu erreichenden Ziele werden durch das Topmanagement vorgegeben.
- » Richtlinien:
Verabschiedung von Sicherheitsrichtlinien (Security Policies), die den sicheren Umgang mit der IT-Infrastruktur und den Informationen definieren.
- » Personalmanagement:
Bei Einstellung, Einarbeitung sowie Beendigung oder Wechsel der Anstellung von Mitarbeitern werden die Anforderungen der Informationssicherheit berücksichtigt.

EIGENSCHAFTEN UND ZIELE EINES ISMS (2)

- » Aktualität des Wissens:
Es wird sichergestellt, dass die Organisation über aktuelles Wissen in Bezug auf Informationssicherheit verfügt.
- » Qualifikation und Fortbildung:
Es wird sichergestellt, dass das Personal seine Verantwortlichkeiten versteht und es für seine Aufgaben geeignet und qualifiziert ist.
- » Adaptive Sicherheit:
Das angestrebte Niveau der Informationssicherheit wird definiert, umgesetzt und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage angepasst (Kontinuierlicher Verbesserungsprozess).

BEKANNTE ISMS (ACHTUNG! SCHLEICHWERBUNG!)

BSI IT-Grundschutz

ISO/IEC 27001

CISIS12

VdS 10000

Aufwand für Umsetzung + Betrieb

INTERMEZZO
ENDE

KONTAKTDATEN

MEINE KONTAKTDATEN

- » Telefon: +49 163 732 74 75
- » Mail: sicherheit [at] mark [minus] semmler [dot] de
- » IM: Threema (ID: VTH4PXRW), Signal, Wire, Telegram
- » Web: <https://www.mark-semmler.de>

**VIELEN DANK FÜR
IHRE AUFMERKSAMKEIT**