- RANSOMWARE -

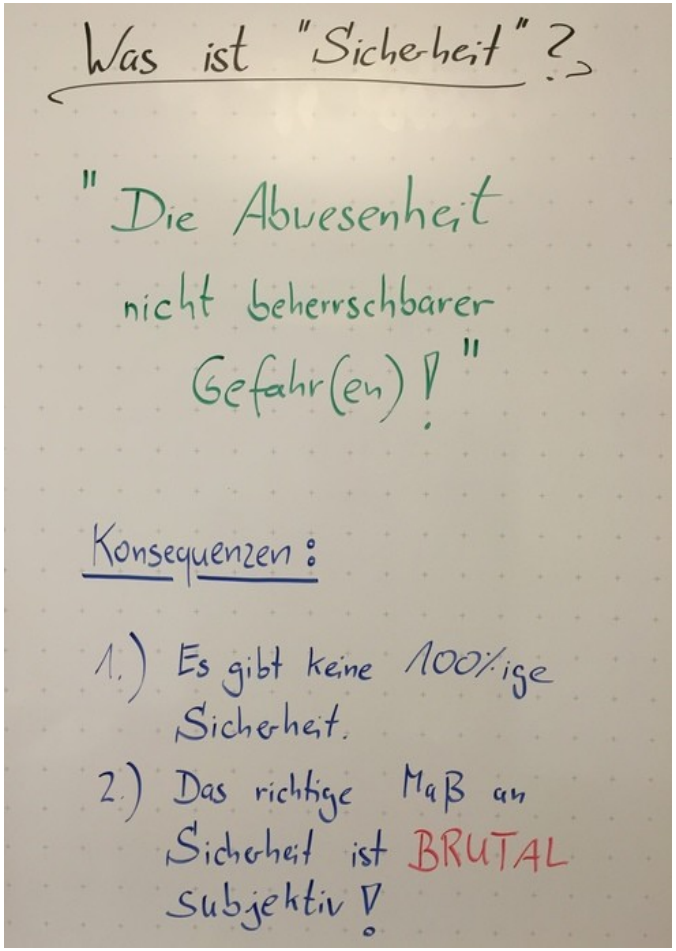
WIE UNTERNEHMEN (UND VERWALTUNGEN) ATTACKIERT WERDEN

Mark Semmler

- EINFÜHRUNG (1) -

GRUNDLAGEN: BEGRIFFE

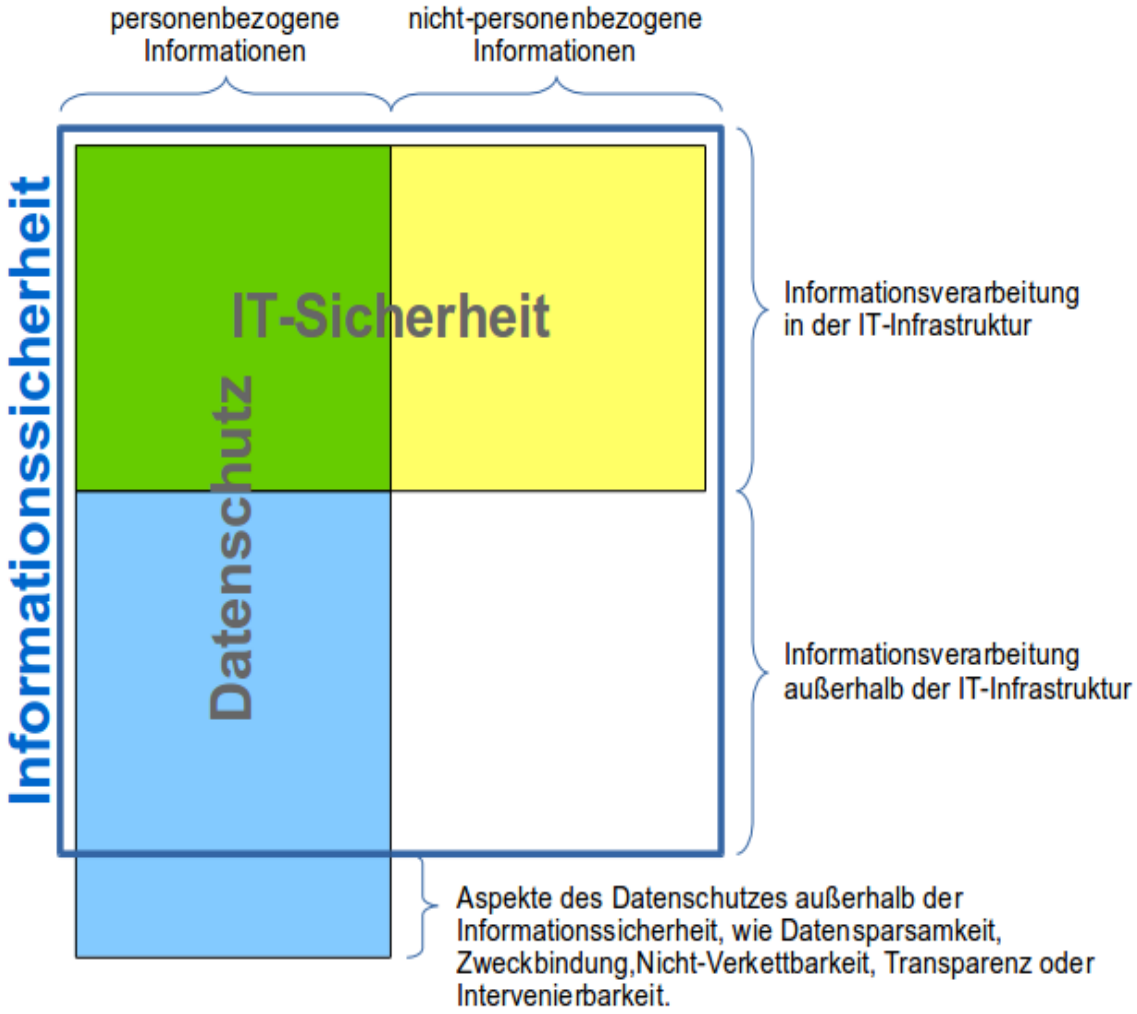
Begriffsdefinition: Was ist Sicherheit?



Die nebenstehende Definition impliziert:

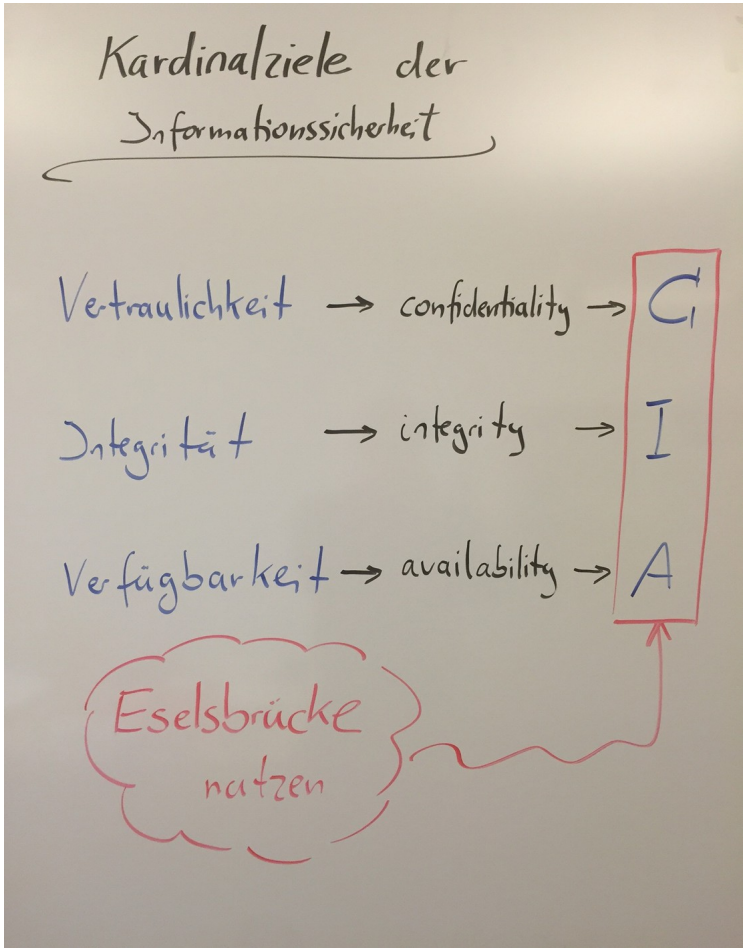
- Wenn Sie sich um (Informations-)Sicherheit kümmern wollen/sollen/müssen, arbeiten Sie vor allem mit Menschen.
- Informationssicherheit ist keine Frage der technischen Ausstattung, sondern ein Teamsport in verschiedenen Disziplinen.
- Diplomatie ist gefragt!
  Sie müssen zuhören, argumentieren, akzeptieren, Kompromisse eingehen.
- Sie sind Techniker, Anwalt und Außenminister in einer Person.

Weitere Begriffe: Informationssicherheit, IT-Sicherheit, Datenschutz



- Informationssicherheit:
  Sicherstellen der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.
- IT-Sicherheit:
  Schutz der elektronischen Informationsverarbeitung. Untermenge der Informationssicherheit.
- Datenschutz:
  Der Schutz des Einzelnen vor Missbrauch seiner personenbezogenen Informationen.

Ziele der Informationssicherheit

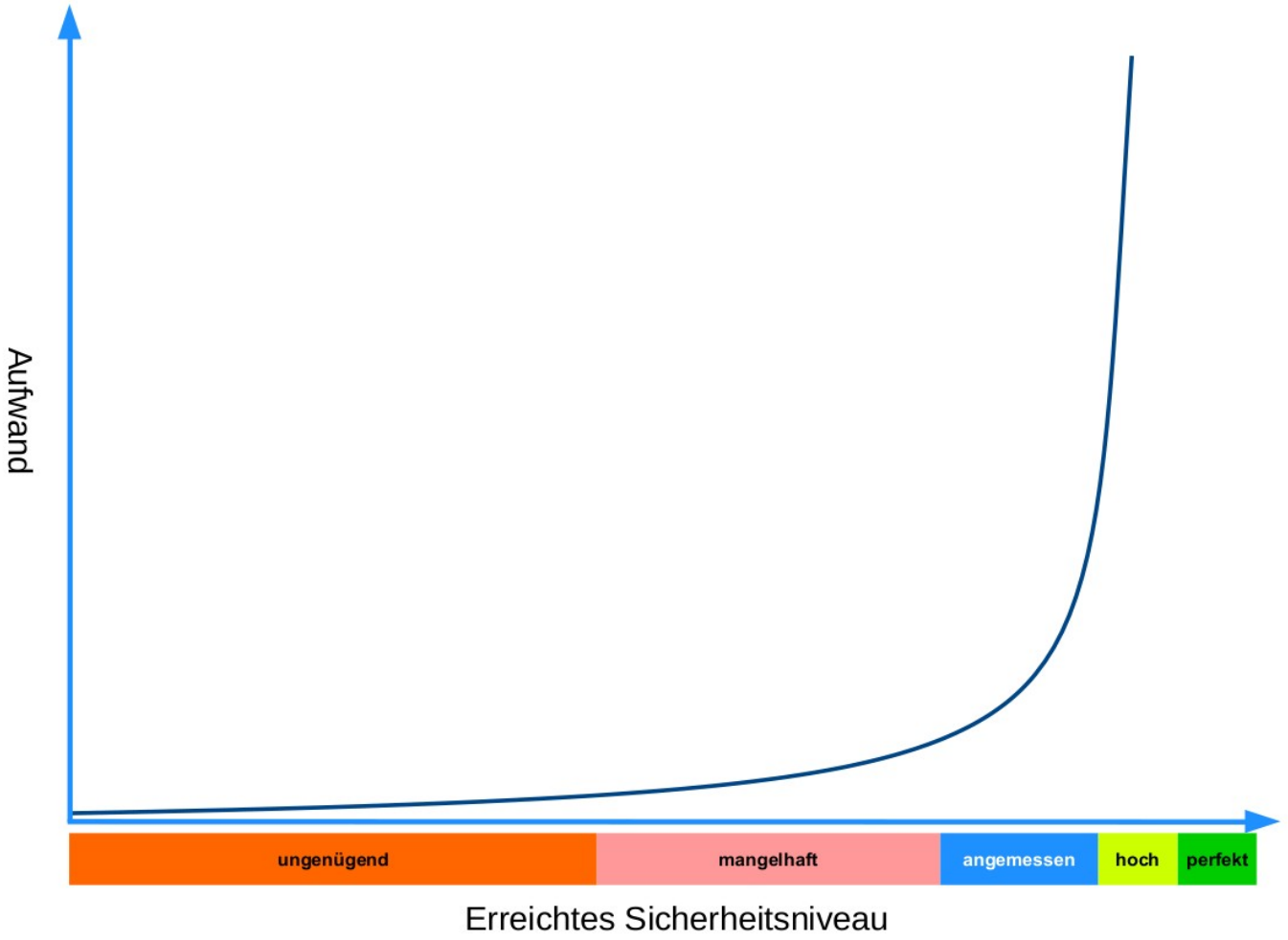


- Vertraulichkeit
  - Nur berechtigte Personen haben lesenden Zugriff.
- Integrität
  - Nur berechtigte Personen haben schreibenden Zugriff und die Informationsverarbeitung ist korrekt (fehlerfrei) abgelaufen.
  - „Ich kann meinen Informationen vertrauen.“
- Verfügbarkeit
  - Die Informationen (und die Informationsverarbeitung) sind da, wenn sie benötigt werden.

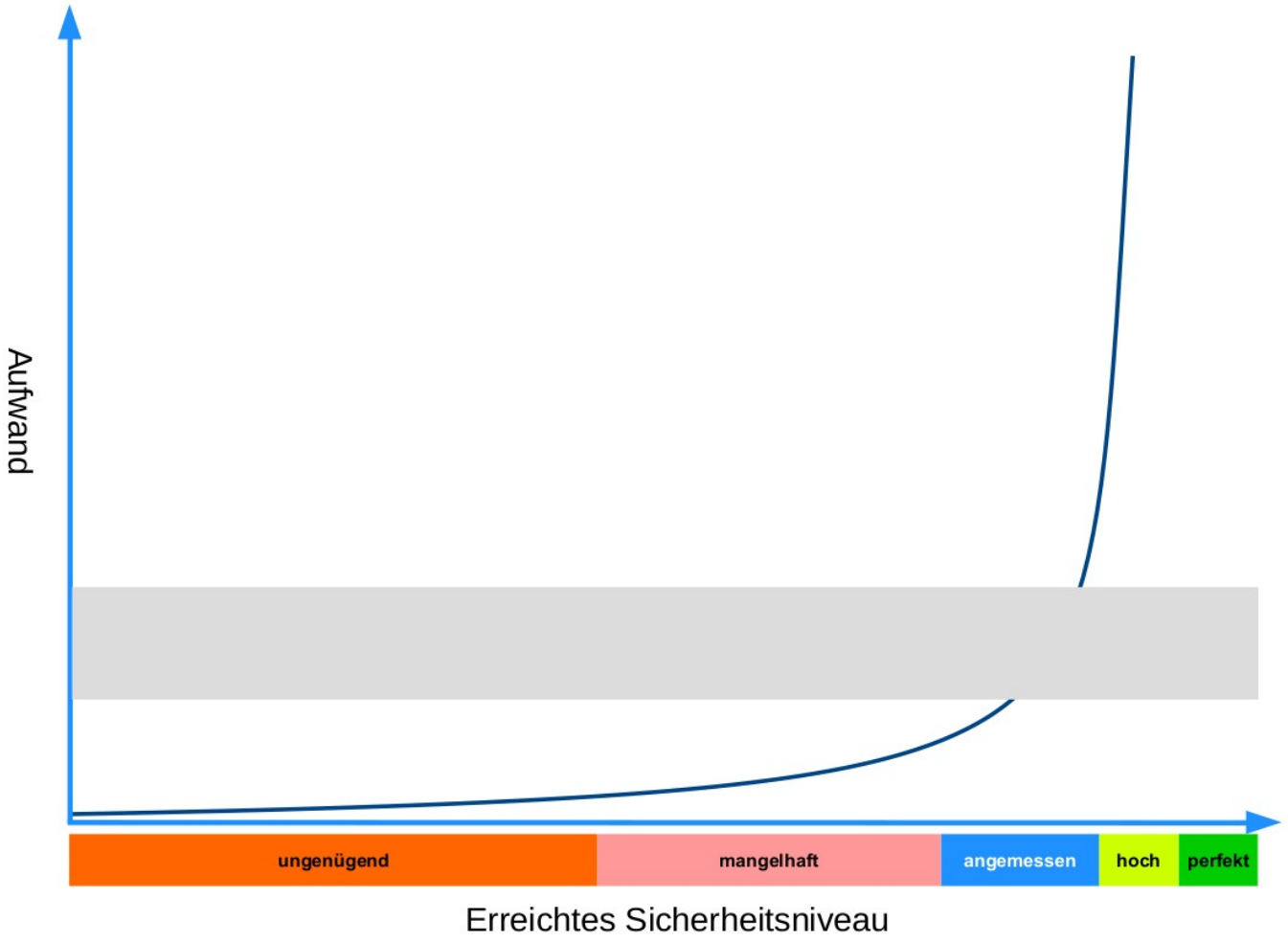
- EINFÜHRUNG (2) -

GUTE SICHERHEIT:
SO WENIG WIE MÖGLICH -
SO VIEL WIE NÖTIG!

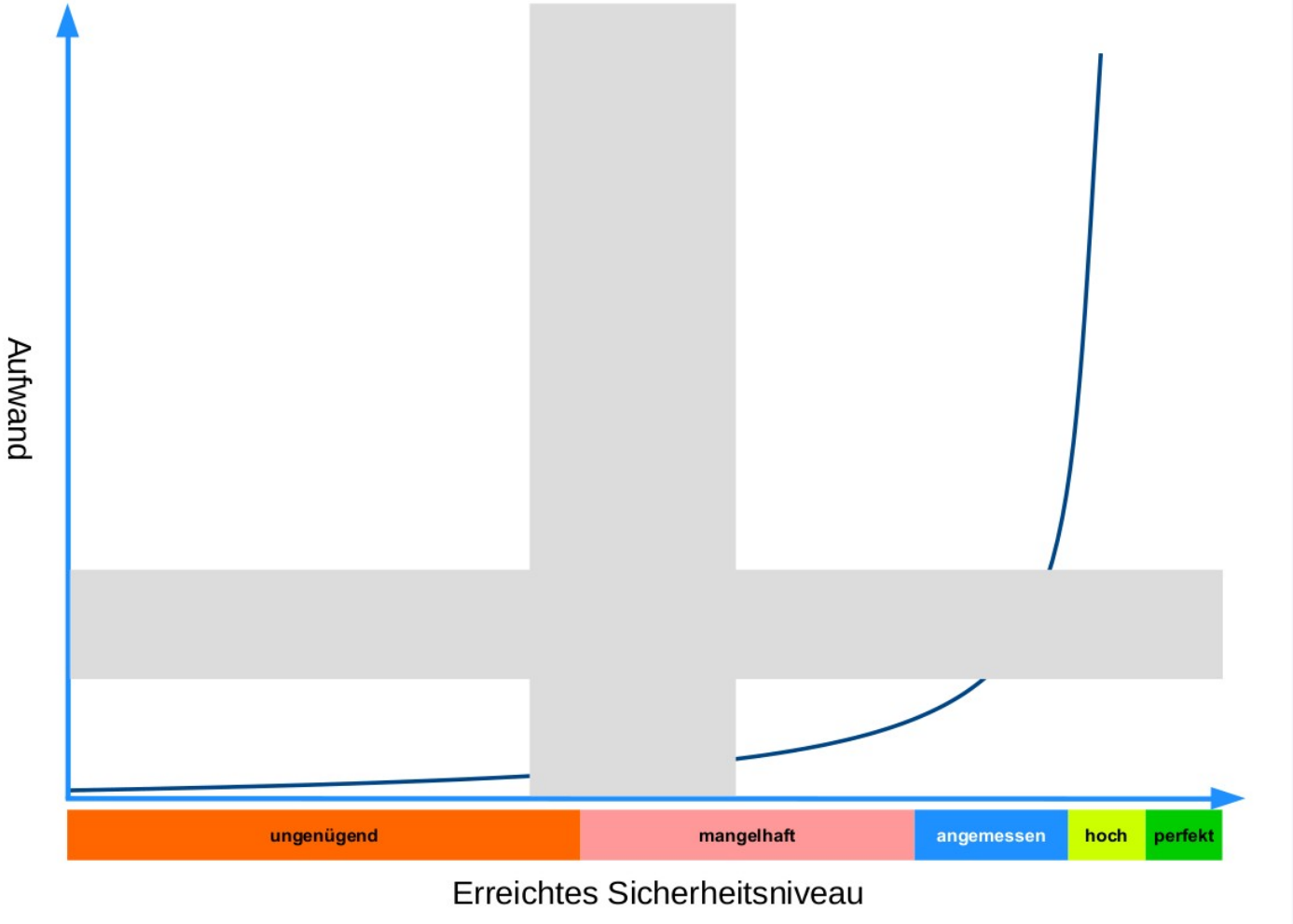
Pareto-Prinzip und Informationssicherheit



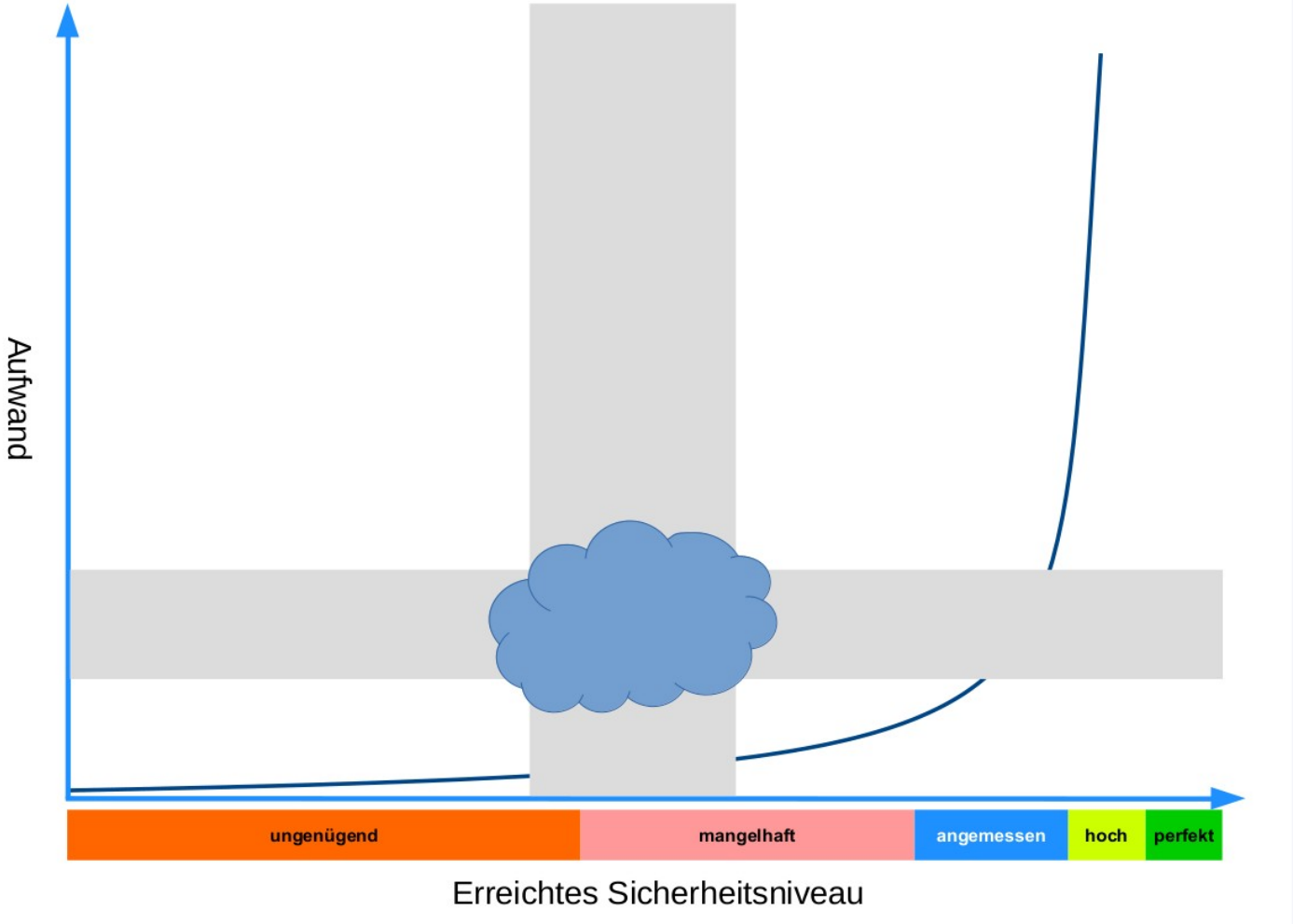
Wie viel Aufwand treiben Sie?



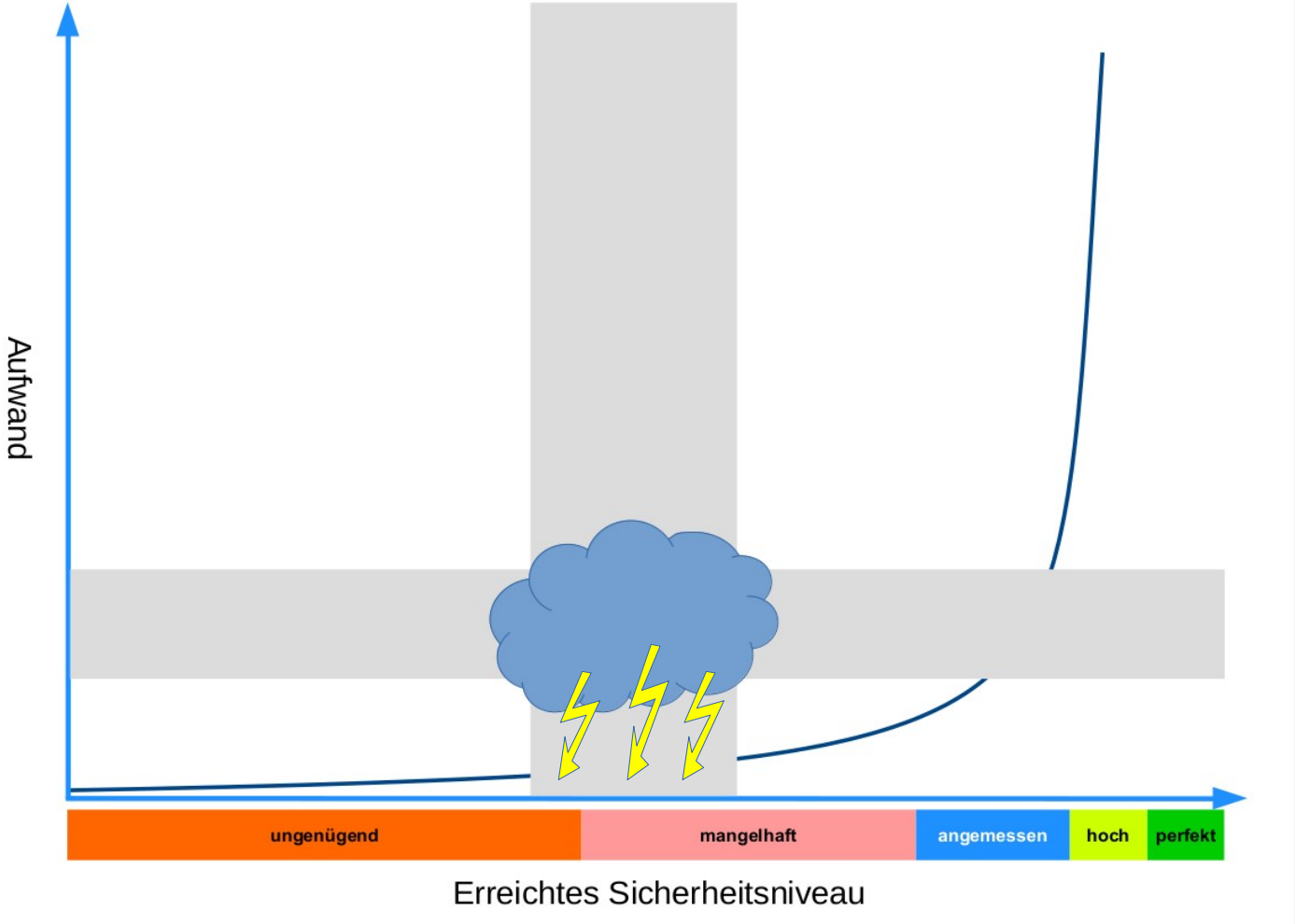
Und wie ist Ihr Sicherheitsniveau?



Sie stehen also ungefähr hier

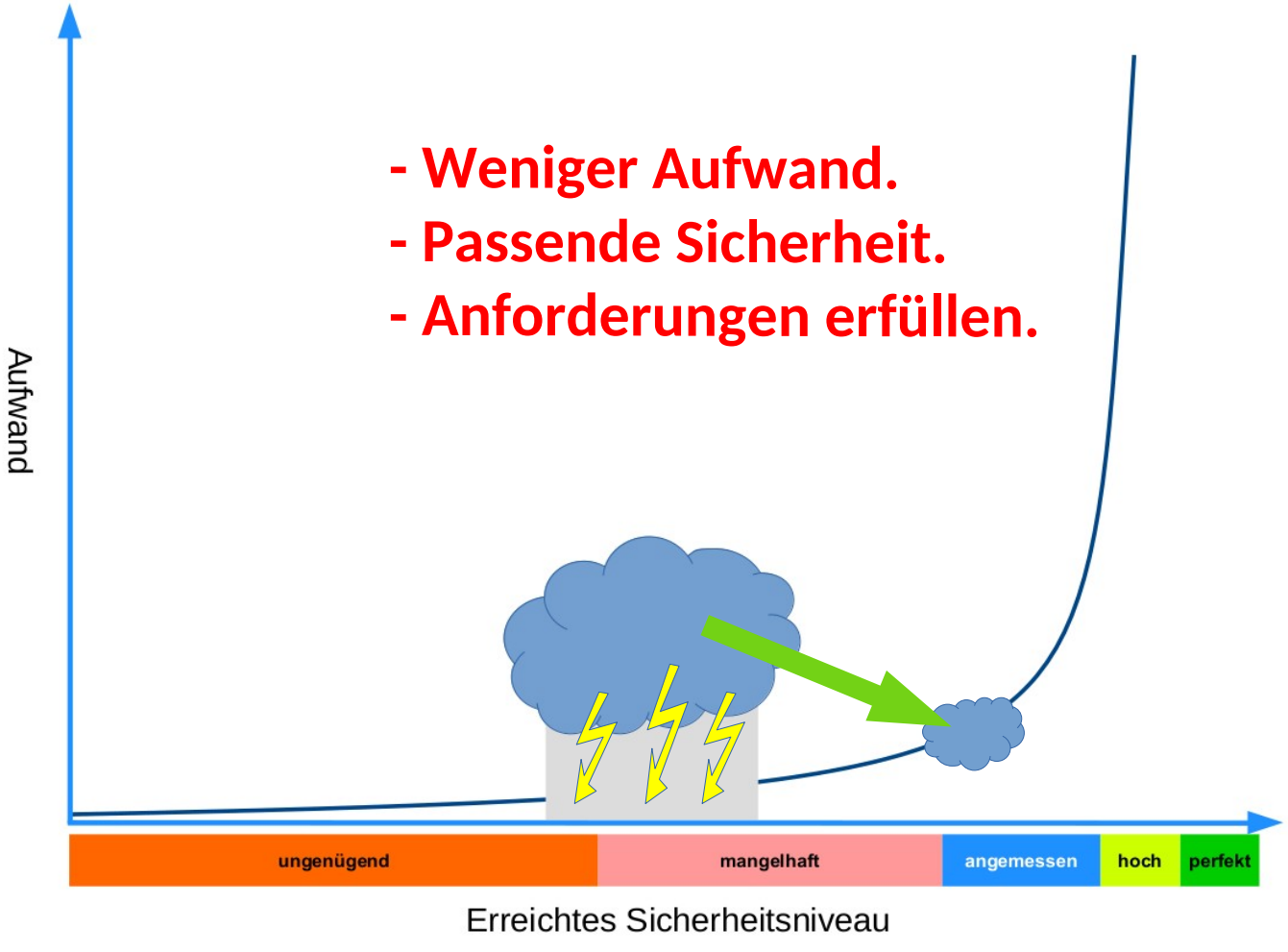


Na ja… Eigentlich stehen Sie hier...

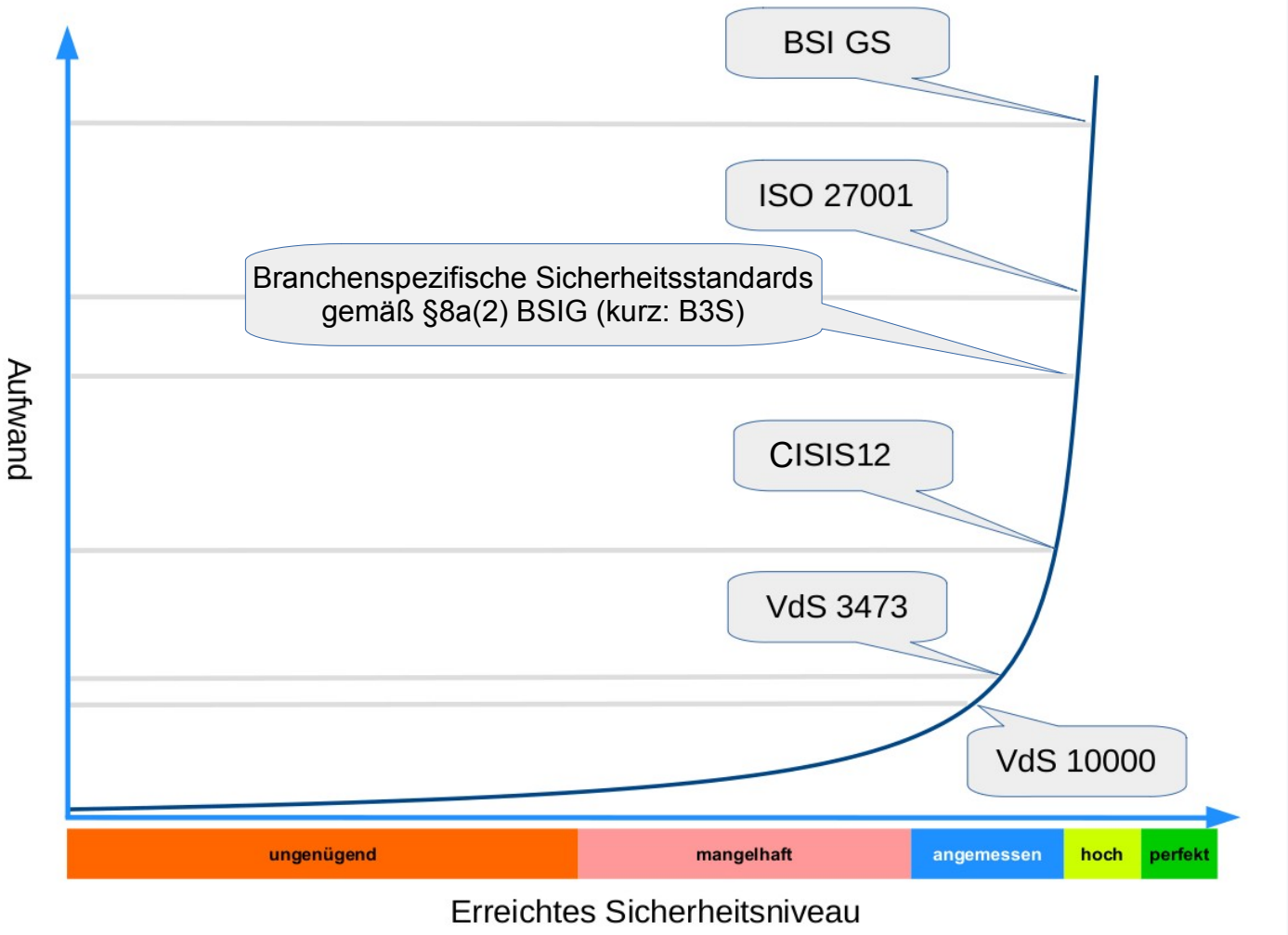


Das hat unangenehme Folgen

Ziel einer angemessenen Absicherung



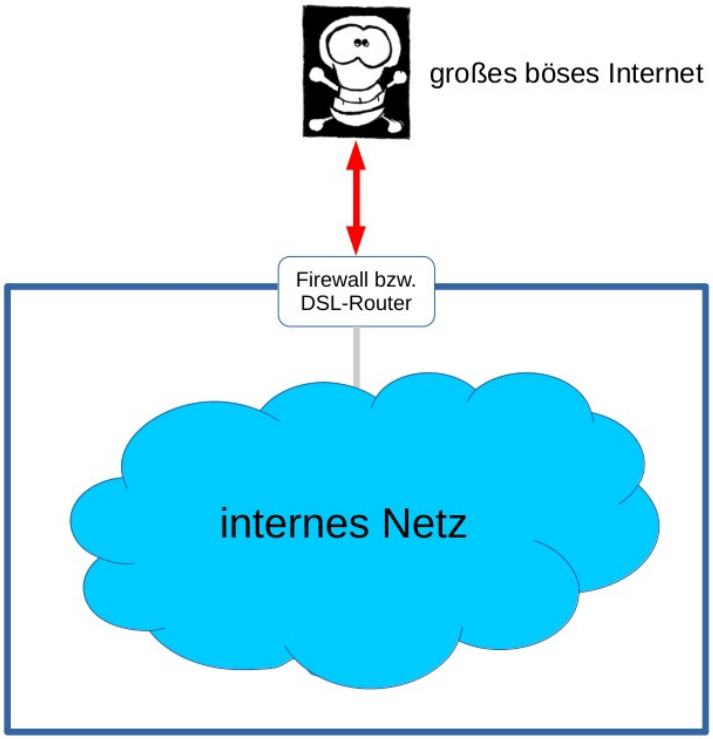
Standards in der Informationssicherheit

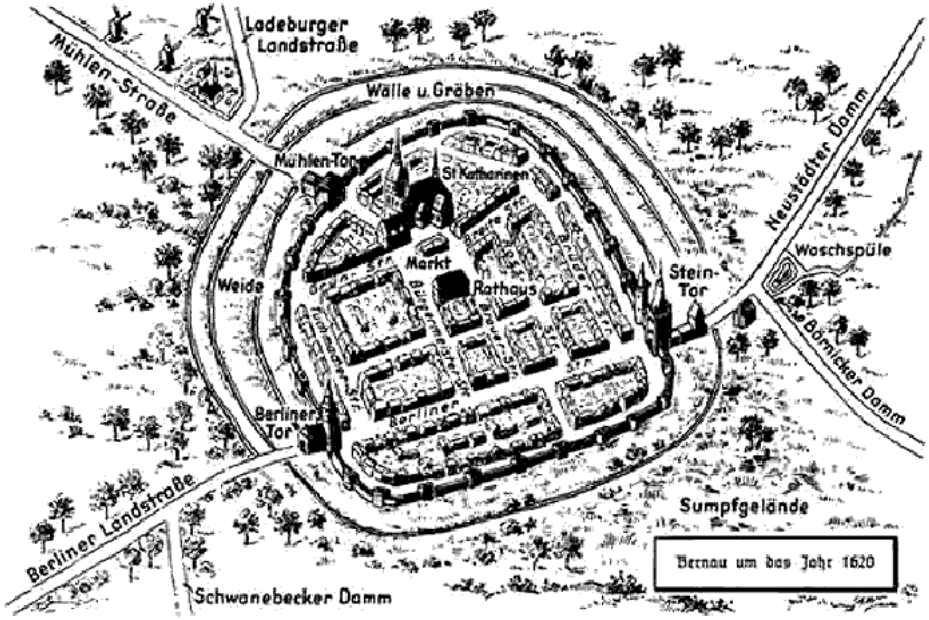


- RANSOMWARE -

WIE UNTERNEHMEN ATTACKIERT WERDEN

WILLKOMMEN IM MITTELALTER (AUFGABE: FINDEN SIE 10 UNTERSCHIEDE)

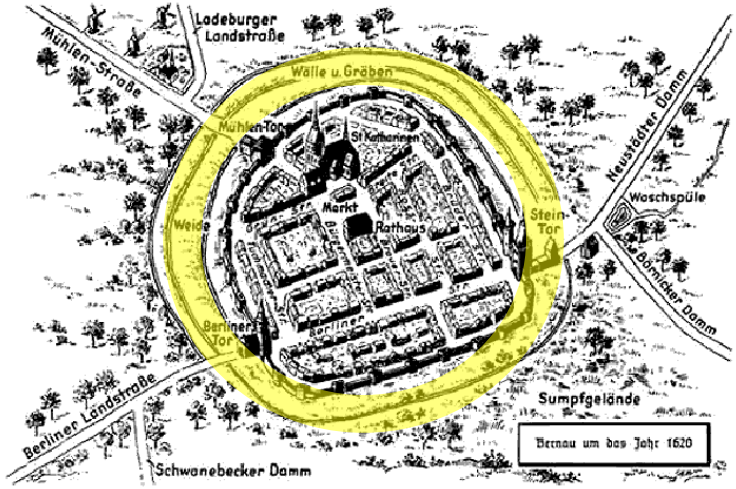




RANSOMWARE-GANGSTER

- Mit Ransomware wird seit Monaten und Jahren sehr viel Geld verdient. Die Akteure sind arbeitsteilig organisiert und verfügen über umfangreiche finanzielle Ressourcen sowie erhebliche kriminelle Energie.
- Auf den nächsten Seiten erhalten Sie eine kurze Übersicht darüber, wie Unternehmen von Ransomware-Gruppen attackiert werden.
- Ransomware-Attacken laufen nicht uniform ab. Die Angreifer wählen ab einem gewissen Punkt individuelle Vorgehensweisen: Abhängig von den Angreifern, der IT-Infrastruktur des Opfers und weiteren Faktoren werden unterschiedliche Strategien und unterschiedliche Automatisierungsgrade beobachtet werden.

1. AKT: STADTMAUER ÜBERWINDEN



SICHERHEIT DURCH TECHNIK? SCHWEIZER KÄSE!

EINFACHE BEUTE: LEICHTSINNIGE ORGANISATIONEN

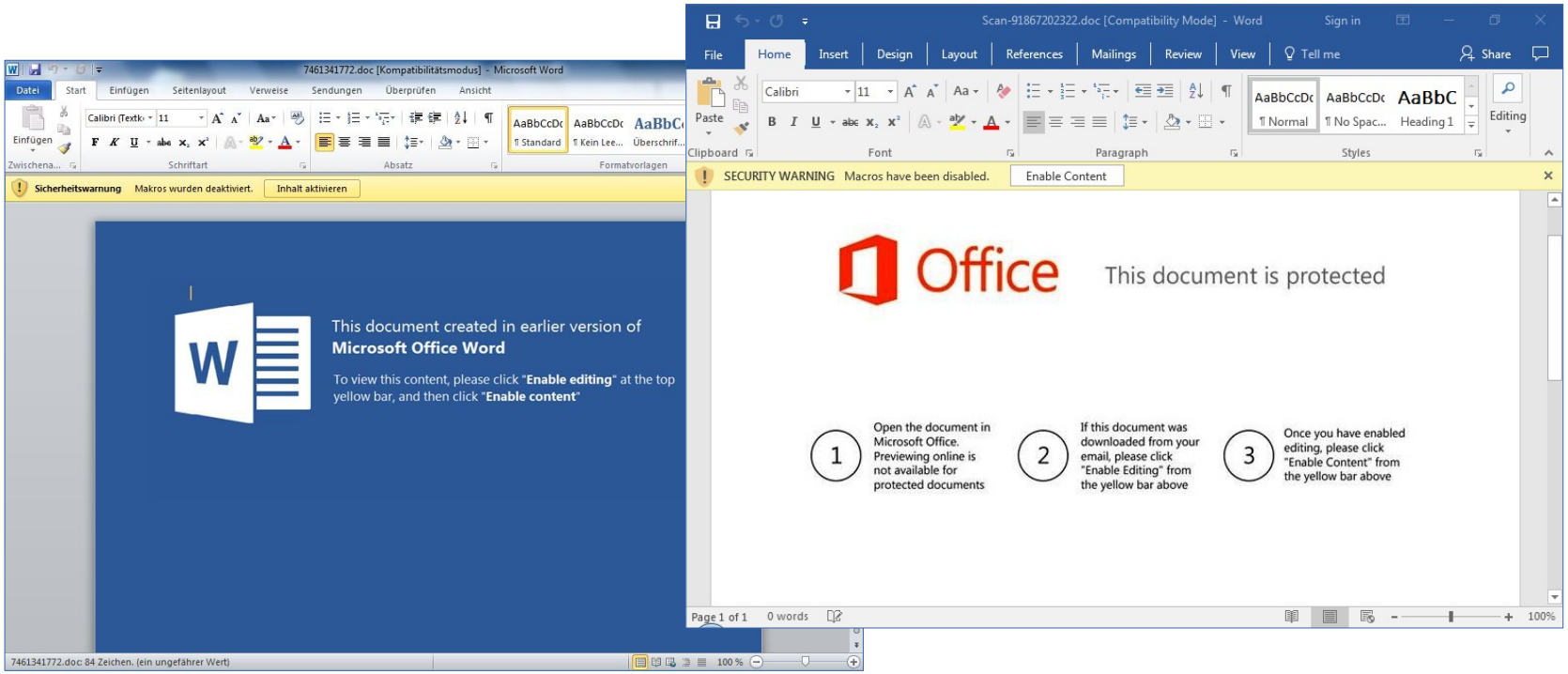
- Die meisten Opfer werden über Massenangriffe gefunden.
- Diese Angriffe richten sich nicht gegen einzelne Unternehmen; vielmehr werden sehr viele potentielle Ziele mit einfachen, wohl bekannten Methoden attackiert.
- Die gebräuchlichsten Attacken sind hier:
  - Platz 1: Schadsoftware in E-Mail-Anhängen
  - Platz 2: Raten von Zugängen
  - Platz 3: Nutzen von Schwachstellen (Exploits)

NICHT JEDER KLICK FÜHRT ZUM ZIEL...

- Mit weitem Abstand sind verseuchte E-Mail-Anhänge der Angriffsvektor Nr. 1.
  - MS Office-Dokumente mit eingebetteten bösartigen Makros (> 95%)
    - MS Word (mit Abstand am häufigsten)
    - MS Excel (gelegentlich)
    - MS Powerpoint (selten)
  - PDF mit eingebetteten Links (sehr selten)
  - sonstige (Anteil verschwindend gering, < 1%)
- Absender, Empfänger, Betreff und Text der E-Mails werden unter Umständen von den Angreifern auf Basis erbeuteter Mails erstellt, um eine höhere Vertrauenswürdigkeit vorzugaukeln.

BEISPIEL: VERSEUCHTES WORD-DOKUMENT

- Nach dem Doppelklick werden die Opfer ggf. durch das Dokument dazu aufgefordert, die Makros („aktive Inhalte“) freizuschalten.



SCHLECHTE PASSWÖRTER? TICKET IN DIE HÖLLE.

- Angreifer versuchen Benutzernamen und Passwörter von IT-Systemen zu erraten, die aus dem Internet erreichbar sind.
- Besonders im Fokus: Remote-Desktop-Lösungen
  - IT-Support: Fernwartungssoftware
  - Homeoffice: Remote-Desktop-Protokoll (RDP) und CITRIX
  - …
- Fun Fact:
  Unter Sicherheitsexperten steht “RDP” nicht mehr für “Remote Desktop Protocol” sondern für “Ransomware Deployment Protocol” :-)

KEINE UPDATES? TÜR STEHT OFFEN.

- Einzelne Gruppen suchen zielgerichtet nach IT-Systemen mit wohl bekannten Sicherheitslücken.
- Unter anderem wurden bereits die folgenden Verwundbarkeiten aktiv ausgenutzt:

LAUFMASCHE: WENN DER WURM DRIN IST...

- Verschiedene Organisationen werden/wurden aufgrund von Sicherheitsproblemen Dritter übernommen.
- Hier nutzen die Angreifer bereits erbeutete Informationen bzw. privilegierte Positionen, um weitere Opfer zu übernehmen.
- Die gebräuchlichsten Attacken sind hier:
  - Platz 1: Nutzen von ausgespähten Zugängen
  - Platz 2: Infektion über vertrauenswürdige Kanäle (Dienstleister)
  - Platz 3: Infektion über vertrauenswürdige Software (Hersteller)

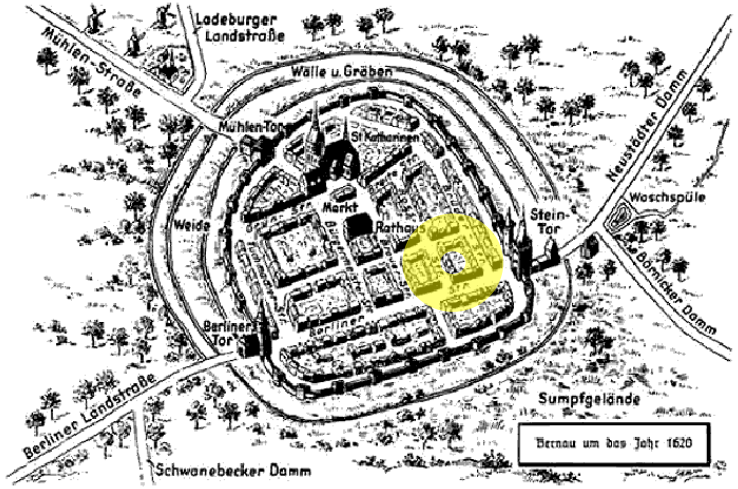
KEINE 2-FAKTOR-AUTHENTIFIZIERUNG? AUA.

- Die Angreifer nutzen ausgespähte Benutzernamen und Passwörter um IT-Systeme zu betreten, die aus dem Internet erreichbar sind.
- Auch hier wieder im Fokus: Remote-Desktop-Lösungen
  - Fernwartungssoftware
  - RDP
  - CITRIX
  - …

WENN DER IT-DIENSTLEISTER PROBLEME HAT

- Zahlenmäßige selten wird Ransomware über vertrauenswürdige Kanäle eingeschleppt.
- Wenn Ransomware-Gangs einen IT-Dienstleister übernommen haben, nutzen sie häufiger dessen Infrastruktur (VPN-Zugänge und/oder sonstige Fernwartungszugänge), um die Kunden des Opfers zu infizieren.
- Die Schäden sind in diesen Fällen sehr hoch, weil z. B. sämtliche Kunden eines IT-Dienstleisters auf einmal betroffen sind.
- ACHTUNG!
  Dienstleister in der Haftung bei (grober) Fahrlässigkeit?!

2. AKT: BRÜCKENKOPF AUFBAUEN



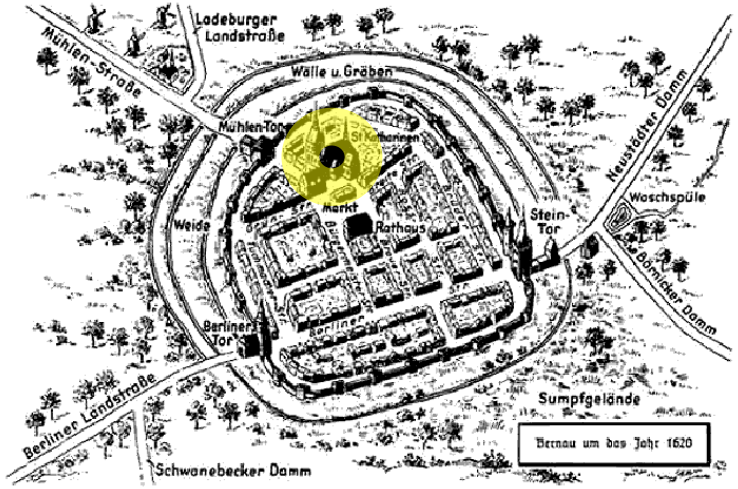
ETABLIEREN IM ERSTEN SYSTEM

- Nachladen verschiedener Module und anschließend automatisiertes Modifizieren des angegriffenen Rechners.
  - Ausweiten der Rechte des Angreifers (falls überhaupt noch nötig).
  - Zugriff absichern.
    - Deaktivieren von Anti-Viren.
    - Deaktivieren von Sicherheitsfunktionen des Betriebssystems (selten).
  - Installieren einer Fernwartung.
    - Nutzen von speziellen „Remote Access Tools“ (RAT) oder Einsatz von „legalen“ Fernwartungstools (Fernwartungstools werden von Anti-Viren i. d. R. nicht als bösartig erkannt).

AUSSPÄHEN DES RECHNERS

- Kopieren der E-Mail-Korrespondenz.
  - Nutzen für die effektive Weiterverbreitung der Schadsoftware via E-Mail in zukünftigen Kampagnen (Absender, Empfänger, Betreff, Inhalte).
- Auslesen der lokal gespeicherten Zugangsdaten.
  - Browser (sehr ergiebige Quelle)
  - Im Arbeitsspeicher zwischengespeicherte Passwörter (hier: Schwachstelle von Microsoft AD → GOLDEN TICKET)

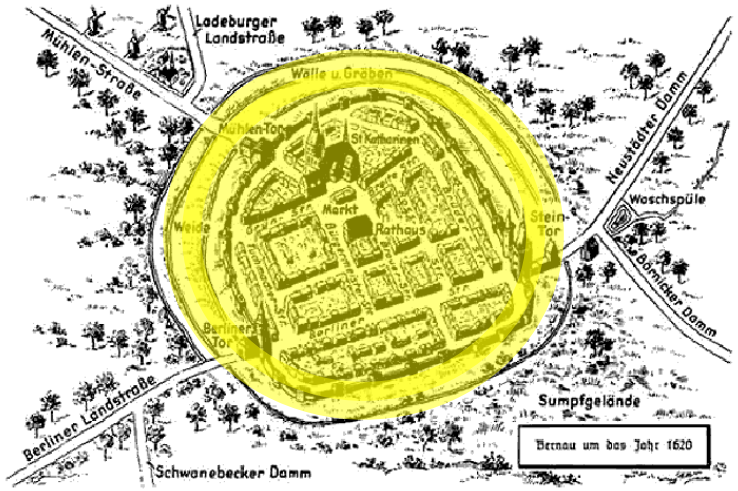
3. AKT: ÜBERNAHME ZENTRALER SYSTEME



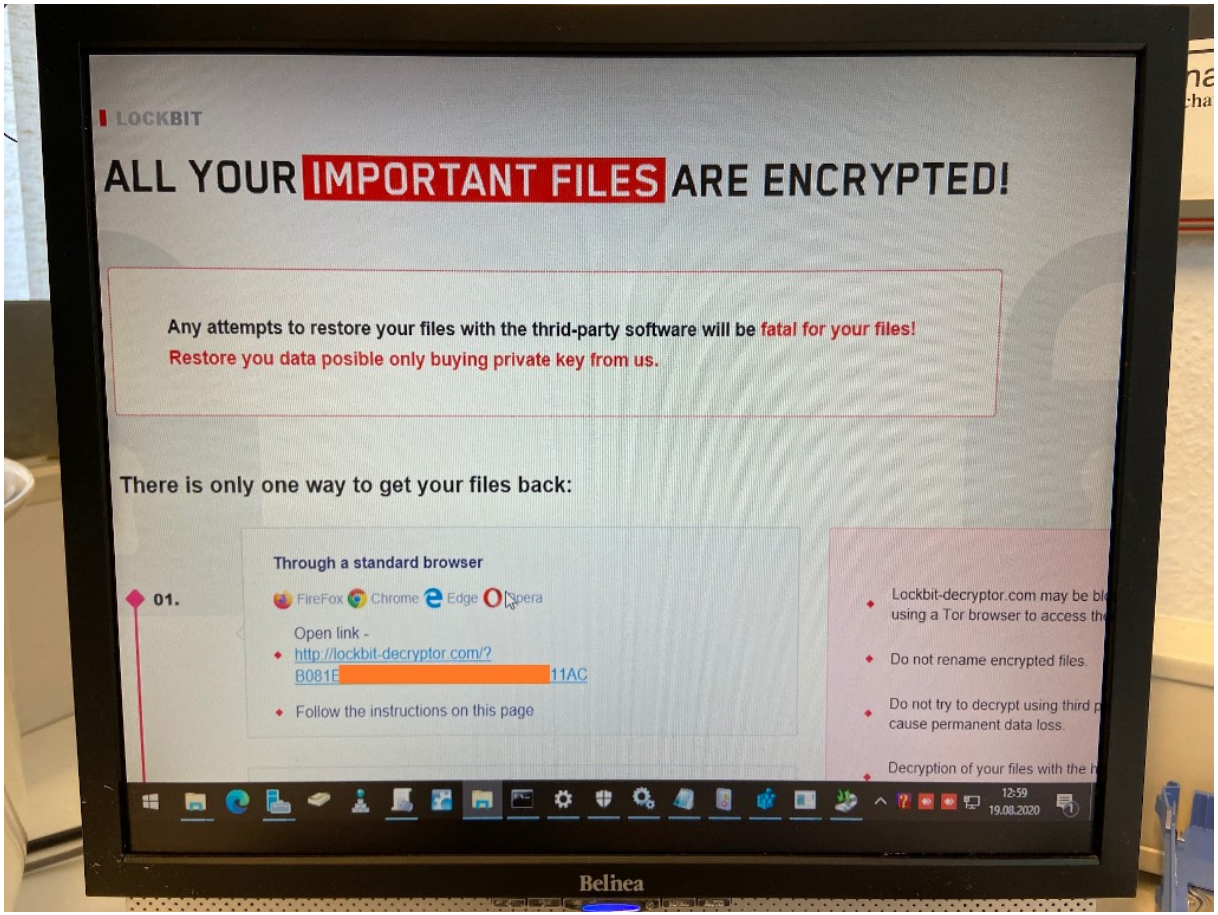
VORGEHENSWEISE

- Übernahme zentraler Systeme des Netzwerks.
  - Ausnutzen unsicherer Konfigurationen (z. B. bei Microsoft AD → GOLDEN TICKET)
  - Raten von Passwörtern
  - Ausnutzen wohlbekannter Schwachstellen
- Hierfür stehen eine Reihe professioneller Tools zur Verfügung (z. B. „CobaltStrike“, siehe https://www.cobaltstrike.com/)
- Das Ziel der Angreifer:
  - Löschen/Sabotage der Datensicherung.
  - Abschalten/Sabotage von Antiviren-Lösungen.
  - Kopieren des Datenbestands.
  - Ausrollen der Verschlüsselungssoftware auf sämtlichen IT-Systemen.
- Die Verschlüsselung geschieht in einer abgestimmten Aktion.
  - Die Verschlüsselungssoftware wird gleichzeitig auf möglichst vielen IT-Systemen gestartet.
  - Sie bleibt auch nach der Verschlüsselung des IT-Systems aktiv, um neu angeschlossene Datenträger (Datensicherung!) zu verschlüsseln.

4. AKT: VERSCHLÜSSELUNG



ES. BRENNT.


LOCKBIT
ALL YOUR IMPORTANT FILES ARE ENCRYPTED!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
Restore you data posible only buying private key from us.
There is only one way to get your files back:
Through a standard browser
01.
FireFox Chrome Edge Opera
Open link -
http://lockbit-decryptor.com/?
B081E 11AC
Follow the instructions on this page
Lockbit-decryptor.com may be bl
using a Tor browser to access th
Do not rename encrypted files.
Do not try to decrypt using third p
cause permanent data loss.
Decryption of your files with the h
12:59
19.08.2020
Belinea

WIE WERDEN DIE DATEN VERSCHLÜSSELT?

- Die Verschlüsselungssoftware…
  - …wird auf sämtliche IT-Systeme ausgerollt und gleichzeitig auf möglichst vielen IT-Systemen gestartet.
  - …bleibt auch nach der Verschlüsselung des IT-Systems aktiv, um neu angeschlossene Datenträger – Datensicherung! – zu verschlüsseln.
  - …wird so im System verankert, dass sie bei jedem Start aktiv wird (eine unterbrochene Verschlüsselung kann so ggf. fortgesetzt werden).
- Die Verschlüsselung nutzt die Public-Key-Kryptografie.
  - Hierbei werden zwei zusammengehörige Schlüssel (Schlüsselpaar) eingesetzt.
  - Es gilt: Alles was mit einem der Schlüssel verschlüsselt wird, kann nur mit dem anderen Schlüssel wieder entschlüsselt werden.
  - Das Schlüsselpaar wird auf dem Server des Angreifers erstellt und nur einer der Schlüssel zum Opfer übertragen. Die Opfer müssen für die Bereitstellung des zweiten Schlüssels zahlen
- Dateien werden häufig nicht komplett verschlüsselt, um möglichst viele Dateien innerhalb einer kurzen Zeit unbrauchbar zu machen (→ Ansatz für Forensik).

HÄUFIG: SCHWACHSTELLEN IN DER RANSOMWARE

- Dateien werden i. d. R. nur teilweise verschlüsselt.
  - Ziel: Schadensmaximierung! Es sollen so möglichst viele Dateien innerhalb einer kurzen Zeit unbrauchbar gemacht werden.
  - Möglichkeiten der forensischen Wiederherstellung!
  - Beispiel: LockBit 2.0 verschlüsselt z. B. nur die ersten 4.096 Byte (4kB) einer Datei.
- Manche (!) Verschlüsselungen sind kryptographisch unsauber entworfen.
  - Grund: Einige Programmierer von Ransomware haben keine Ahnung von Kryptografie.
  - Möglichkeiten der Entschlüsselung.
  - Beispiel: HIVE arbeitet mit so genannten Keystreams, die unsauber erzeugt werden.
- Manche Verschlüsselungen sind so schlecht programmiert, dass Dateien zerstört werden.
  - Grund: Einige Programmierer von Ransomware haben keine Ahnung von guter Programmierung.
  - Beispiel: ONYX kommt mit großen Dateien nicht zurecht und zerstört sie.

DIE FOLGEN

Mühlen-Straße
Neustädter Damm
Stein-Tor
Bärnicker Damm
Sumpfgelände
Berliner Landstraße
Schwanebecker Damm
Bernau um das Jahr 1620

DIE SCHÄDEN SIND EXISTENZBEDROHEND (1)

- Abrupte und vollständige Betriebsunterbrechung
  - Server, Clients, Telefonanlage, Zeiterfassung, … – die gesamte IT steht still.
  - Merke:
    - Ohne IT keine Prozesse.
    - Ohne IT keine Verwaltung/Produktion/Entwicklung.
- Backups sind ggf. nicht mehr existent oder nicht aktuell.
  - Wiederherstellung???
  - Datenverlust?!
- Die Angreifer haben vertrauliche/sensible Daten kopiert.
  - Die Angreifer drohen mit der Veröffentlichung.
  - Sie müssen ggf. Aufsichtbehörden, Kunden, etc. informieren.
    - Peinlich? Sehr.
    - Rechtliche Folgen?!

DIE SCHÄDEN SIND EXISTENZBEDROHEND (2)

- Lösegeld.
  - Das kleinste Stück vom Kuchen.
- Intensive Unterstützung wird benötigt.
  - Ersthelfer
  - intensiver IT-Support
  - IT-Forensiker
- Im Nachgang:
  - Sie können Ihrer IT nicht mehr vertrauen.
    - Neuinstallation aller IT-Systeme?!
    - Härten der IT-Systeme.
  - Zerstörtes Vertrauen in der Organisation.
    - Leistungsträger kündigen.
    - Führungskräfte (IT-Leiter, …) werden gekündigt.
    - Häufig ist die Produktivität über Wochen und Monate hinweg eingeschränkt.

ACHTUNG! ES GIBT GGF. WEITERE SCHÄDEN/RISIKEN!

- Keine Entschlüsselung trotz Zahlung des Lösegelds.
  - I. d. R. (> 95%) erhalten die Betroffenen nach Zahlung des Lösegelds das entsprechende Entschlüsselungsprogramm (und den benötigten Schlüssel).
  - In einigen Fällen wird jedoch nicht geliefert und das betroffene Unternehmen hat den doppelten Schaden.
- Zerstörter Datenbestand möglich.
  - Einige Ransomware-Tools sind buggy und zerstören Dateien bei der Verschlüsselung.
  - Wenn mehrere Ransomware-Gruppen das Unternehmen zeitgleich attackieren ist Chaos häufiger vorprogrammiert.
- Entschlüsselungstools arbeiten z. T. sehr langsam.
  - Entschlüsselungszeiten von mehr als zwei Wochen (!) möglich.
  - Beispiel: RYUK kommt mit vielen kleinen Dateien nicht gut zurecht, da zunächst eine Datenbank angelegt und dann die Dateien entschlüsselt werden. Die Datenbank ist schlecht programmiert. Das Entschlüsselungstool arbeitet sehr langsam und stürzt permanent ab.
  - Technischer Support durch die Gangster z. T. extrem schlecht.

- RANSOMWARE -

VORBEUGUNG

DIE DREI ERKENNTNISSE DES TAGES: DIE GESCHÄFTSFÜHRUNG IST VERANTWORTLICH!

- Wer trägt die Verantwortung für die Informationssicherheit?
  - Der Administrator? NEIN!
  - Der externe Dienstleister? NEIN!
  - Der IT-Leiter? NEIN!
  - Der Datenschutzbeauftragte? NEIN!
- Nur die Geschäftsführung ist verantwortlich.
  - Nehmen Sie diese Verantwortung wahr.
  - Kümmern Sie sich! (Keine Angst – das ist kein Hexenwerk!)
  - Alles andere ist grob fahrlässig.

KEINE KOMPROMISSE BEI DER DATENSICHERUNG! (1)

- Hier die organisatorischen Aufgaben:
  - Lassen Sie herausfinden, wo Ihre wichtigsten Daten gespeichert sind.
  - Legen Sie zusätzlich verbindlich fest, wo Ihre Mitarbeiter Daten speichern dürfen bzw. müssen.
  - Fordern Sie: Diese Speicherorte müssen gesichert werden!
  - Legen Sie die Intervalle der Datensicherungen fest.
    - Empfehlung: Speicherorte sollten so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist.
  - Lassen Sie Ihre Administratoren/Dienstleister die Vorgehensweisen für die Datensicherung und -wiederherstellung der Speicherorte ausarbeiten und dokumentieren (Datensicherungsplan und Wiederanlaufplan).
  - Fordern Sie, dass einmal jährlich ein gesichertes IT-System nach dem Zufallsprinzip ausgewählt und in einer Testumgebung wiederhergestellt wird.
    - Diese Tests sollten anhand des vorliegenden Wiederanlaufplans bewältigt werden.

KEINE KOMPROMISSE BEI DER DATENSICHERUNG! (2)

- So sollte Ihre Datensicherung technisch aussehen:
  - Die für die Datensicherung genutzten IT-Systeme müssen vom restlichen Netz möglichst komplett getrennt sein.
    - Minimal: Die administrativen Zugänge dieser IT-Systeme werden unabhängig von der restlichen IT verwaltet und verfügen über eigene, exklusive Authentifizierungsmerkmale.
    - Optimal: Die IT-Systeme sind vom Rest des Netzes durch eine Firewall/NAT-Device vollständig getrennt.
    - Ziel: Selbst wenn das Produktivnetz komplett unter der Kontrolle von Angreifern steht, bleibt die Datensicherung sicher. Sie kann nicht gelöscht, verschlüsselt oder sabotiert werden.
  - Die gesicherten Daten werden nicht im gleichen Brandabschnitt wie die gesicherten IT-Systeme aufbewahrt.
  - Datensicherungen werden an mehr als einem Standort gelagert, damit die gesicherten Daten auch bei größeren Schadensereignissen verfügbar bleiben.
  - Die Datensicherung wird nach dem Mehr-Generationen-Prinzip (z. B. zusätzliche Jahres-, Monats- und Wochensicherungen) durchgeführt, um die Wahrscheinlichkeit eines umfangreichen Datenverlusts weiter zu verringern.

EFFEKTIV UND EFFIZIENT: KLARE REGELN!

- Die größte Schwachstelle sitzt ca. 50cm vor dem Bildschirm.
  Mitarbeiter benötigen klare Regeln, was in der IT erlaubt und was verboten ist:
  - Definieren Sie, wo die Mitarbeiter die Daten des Unternehmens dauerhaft ablegen müssen.
  - Untersagen Sie das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt, strafrechtlich relevant oder sittenwidrig sind.
  - Legen Sie fest, ob die private Nutzung der IT erlaubt ist und gestalten Sie die Privatnutzung nach den Bedürfnissen des Unternehmens aus.
  - Bestimmen Sie, dass fremde Hard- und Software in der IT-Infrastruktur nichts verloren hat.
  - Untersagen Sie die in der IT-Infrastruktur installierten Sicherheitseinrichtungen zu deinstallieren, zu deaktivieren, mutwillig zu umgehen oder in ihrer Konfiguration zu verändern.
  - Regeln Sie, ob und wann auf den Datenbestand von abwesenden Mitarbeitern zugegriffen werden darf.

DIE 3 SCHLÜSSEL ZU IHREN DIGITALEN WERTEN: MITARBEITER, ZUGÄNGE, ZUGRIFFSRECHTE

- Mitarbeiter, Zugänge und Zugriffsrechte erlauben es, auf ihre nichtöffentliche IT und ihre Informationen zuzugreifen.
- Eine strukturierte Verwaltung ist notwendig und schnell eingerichtet:
  - Im Rahmen der Einarbeitung werden neue Mitarbeiter in die Regelungen der Informationssicherheit eingewiesen.
  - Bei Beendigung oder Wechsel einer Anstellung werden die Zugänge und Zugriffsrechte des Mitarbeiters umgehend überprüft und bei Bedarf angepasst.
  - Mitarbeiter erhalten nur jene Zugänge und Zugangsrechte, die sie für ihre Aufgabenerfüllung benötigen.
  - Zugriffe auf nichtöffentliche Bereiche der IT werden durch geeignete Anmeldeverfahren abgesichert, die eine Authentifizierung verlangen.

VOM SCHAF ZUM STAHLWOLLSCHAF: BASISSCHUTZ FÜR ALLE IT-SYSTEME

- Sämtliche IT-Systeme müssen über ein Mindestmaß an Sicherheitsmaßnahmen verfügen. Stellen Sie mindestens die folgenden Punkte sicher:
  - Verfügbare Sicherheitsupdates für System- und Anwendungssoftware werden installiert (kritische Updates umgehend, bei anderen kann man sich Zeit lassen).
  - IT-Systeme werden vom Rest des Netzes möglichst weit getrennt, wenn sie über Schwachstellen verfügen, die nicht behoben werden (z. B. wenn keine Sicherheitsupdates installiert werden können, Passwörter nicht geändert werden können oder unsichere technische Verfahren eingesetzt werden) oder wenn sie aus dem Internet erreichbar sind.
  - An- und Abmelden von Nutzern, Fehler und Informationssicherheitsereignisse werden protokolliert (wenn möglich auf ein zentrales IT-System).
  - Windows-Systeme werden durch eine Anti-Viren-Software geschützt.
  - Normale Nutzer besitzen keine Administratorrechte.

ZUGRIFFE AUS DEM INTERNET

- IT-Infrastruktur, die im Internet exponiert ist muss speziell geschützt werden.
  - IT-Systeme und Dienste werden nur im Internet zur Verfügung gestellt, wenn dies absolut notwendig ist.
  - Mitarbeiter loggen sich ausschließlich via VPN und/oder 2-Faktor-Authentifizierung ein.
  - Im Internet exponierte IT-Systeme sind vom restlichen Unternehmensnetz möglichst komplett abgekoppelt.
    - Niemals Port-Forwarding vom Internet ins interne Netz erlauben!
    - Ausnahmslos alle exponierten IT-Systeme in die DMZ!

(FAST) ZUM SCHLUSS: EIN PAAR OFFENE WORTE

- Die Maßnahmen der letzten Seiten stellen ein absolutes Mindestmaß dar. Viele wichtige Bereiche (wie z. B. der Umgang mit Smartphones, USB-Sticks oder Cloud-Computing) sind nicht erfasst.
- Durch die Maßnahmen der letzten Seiten arbeiten Sie zumindest nicht mehr grob fahrlässig. Sie besitzen aber dennoch ein (erhebliches) Restrisiko.
- Wer es richtig machen möchte:
  - VdS 10000 für KMU und Verwaltungen
  - VdS 10005 für Klein- und Kleinstunternehmen
- Aus Gründen der Transparenz:
  Der Referent war der Projektleiter bei der Erstellung der genannten Richtlinien.

- RANSOMWARE -

UNMITTELBARE REAKTION

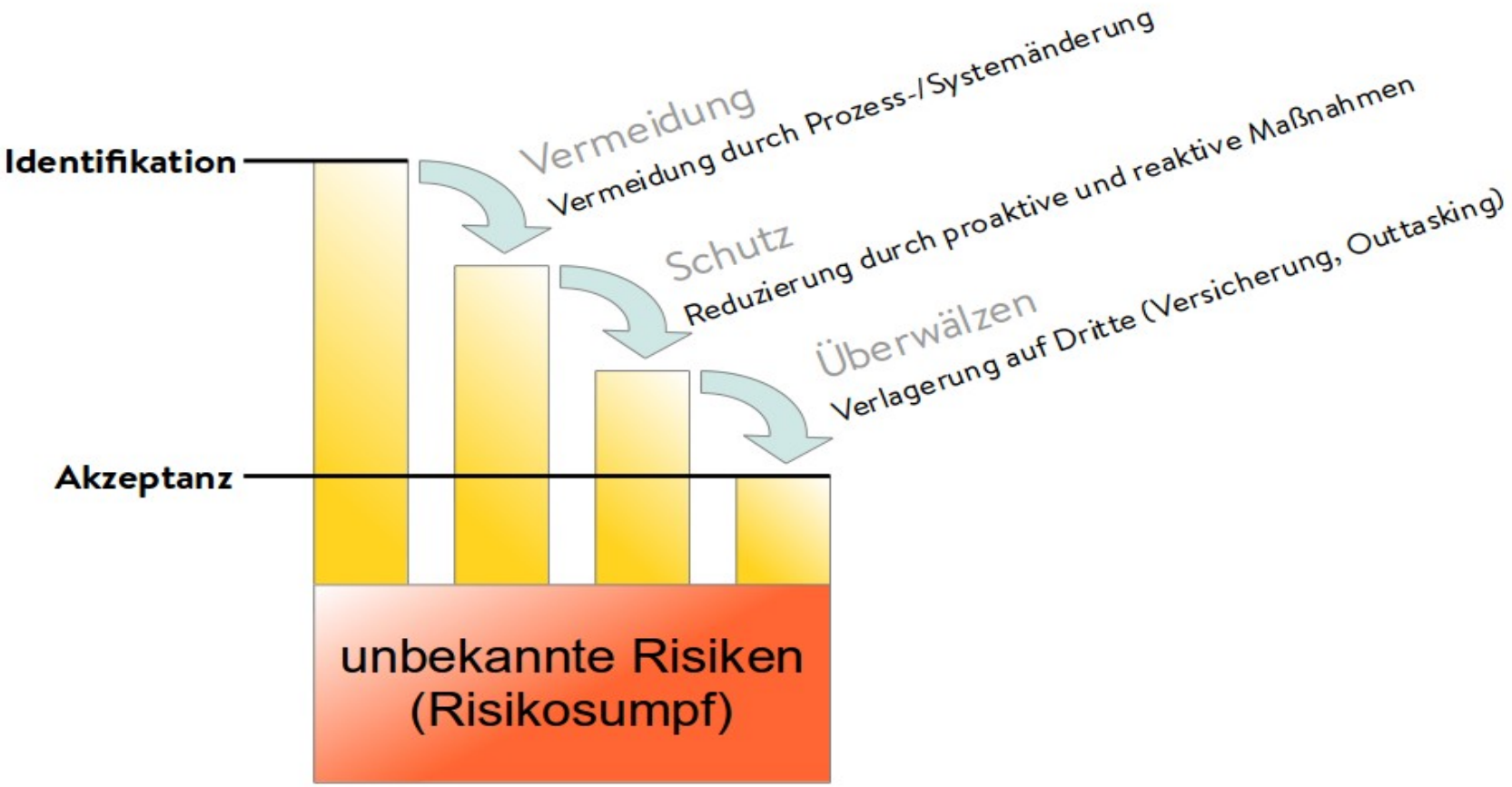
WAS TUN, WENN RANSOMWARE ZUSCHLÄGT?

- Alle Systeme sofort ausschalten (Stecker ziehen).
- Backups vom Netz trennen (wenn möglich zeitgleich mit Schritt 1).
- Spezialisten anrufen.
  - Erster Ansprechpartner: Versicherung
  - Wenn keine Versicherung: IT-Systemhaus
- Goldene Regel:
  - Vor einem Rettungs- oder Entschlüsselungsversuch sollte unbedingt von allen betroffenen IT-Systemen ein Vollbackup durchgeführt werden.

- RANSOMWARE -

CYBER-VERSICHERUNG

RISIKOMANAGEMENT!



NICHT BEHERRSCHBARE RISIKEN KANN/SOLLTE/MUSS MAN ABWÄLZEN.

VORTEILE EINER CYBER-VERSICHERUNG

- Schadensverhütung durch Obliegenheitspflichten.
- Unterstützungsleistungen im Schadensfall.
  - Im Falle eines Falles stehen bei guten Versicherungen Spezialisten umgehend bereit.
- Ausgleich der entstandenen Schäden.
  - Erste Hilfe
  - Kommunikation mit den Erpressern
  - Betriebsunterbrechung
  - Wiederaufbau der IT-Infrastruktur
  - ...

EIN OFFENES WORT:

ALS ERSTHELFER BIN ICH IMMER SEHR, SEHR FROH WENN DER KUNDE EINE CYBER-VERSICHERUNG IM RÜCKEN HAT!

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

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