Niedersächsisches Ministerium
für Inneres und Sport

Verfassungsschutz

Mittelstand trifft Mittelstand, 12.05.2022

Risiken in einer vernetzten Welt

Markus Böger

Verfassungsschutz Niedersachsen - Wirtschaftsschutz

+49 511 6709-284

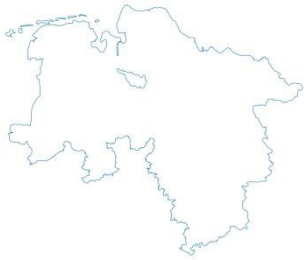
+49 172 4265468

markus.boeger@mi.niedersachsen.de

Warum machen wir das?

Damit Sie auch morgen noch kraftvoll zubeißen können

„Wirtschaftsschutz ist nicht *(oder mehr als)* Cyberschutz“



something about…

Betroffene Unternehmen (Diebstahl, Spionage, …) in den letzten 4 Jahren von gut 50 % auf knapp 90 % gestiegen

60 % mussten innerhalb der letzten 12 Monate auf einen Cyberangriff reagieren *(ohne automatisiert abgewiesene Angriffe)*

Cyberattacken allgemein zugenommen, besonders Malware inkl. Ransomware, DDoS

Schadprogramme +22 % | Daten-Leak-Seiten +360 %

Schadenshöhen enorm gestiegen: Vervielfachung bei Ausfall von Betriebs-/Produktionsabläufen sowie Erpressung – treibende Faktoren!

Nach wie vor...

…glauben viele, es wird sie nicht treffen

…haben viele keinen Notfallplan

…sind viele überfordert

…sagen viele „ja, wir müssten“ – machen aber nicht

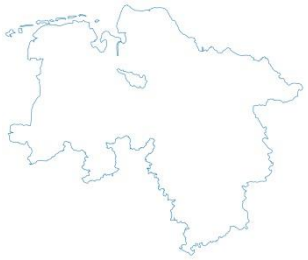
Nach wie vor...

…hat sich an grundlegenden Risiken nichts geändert

E-Mail, Fehlkonfiguration, veraltete Software, fehlende Sensibilisierung, …

…hat sich an grundlegenden Maßnahmen nichts geändert

Backup, Verschlüsselung, Segmentierung, Patchmanagement, Schulung, Monitoring, Notfallplan, […], Versicherung?, …



https://www1.wdr.de/nachrichten/ruhrgebiet/wittener-stadtverwaltung-weiterhin-offline-100.html

Details zu dem Angriff bekannt:

Die Stadt spricht von einer wohl neuen professionellen Gruppe, deren Art von Angriff auch recht neu sein soll. Die Hacker haben offenbar eine Schadsoftware ins Netz eingeschleust. Wie sie das geschafft haben, ist bisher aber unklar.

https://www1.wdr.de/nachrichten/ruhrgebiet/wittener-stadtverwaltung-weiterhin-offline-100.html

Details zu dem Angriff bekannt:

Die Stadt spricht von einer wohl neuen professionellen Gruppe, deren Art von Angriff auch recht neu sein soll. Die Hacker haben offenbar eine Schadsoftware ins Netz eingeschleust. Wie sie das geschafft haben, ist bisher aber unklar.

Als Bürodeutschland am Montagmorgen die Rechner hochfuhr, blinkte auf vielen Bildschirmen eine Warnmeldung: „Öffnen Sie bis auf weiteres KEINE E-Mail-Anhänge von unbekannten Quellen und seien Sie auch ansonsten sehr aufmerksam beim Surfen im Internet."

Emotet

Infrastruktur von Emotet abgeschaltet

Strafverfolger stoppen die gefährlichste Schadsoftware der Welt

Deutschen Ermittlern ist zusammen mit internationalen Partnern ein spektakulärer Schlag gegen die Betreiber der berüchtigten Schadsoftware Emotet gelungen. Ob der Erfolg von Dauer ist, muss sich aber erst zeigen.

Von **Patrick Beuth**
27.01.2021, 17.29 Uhr

…und nun?

Auch nach der Verhaftung von El Chapo (und auch seiner Ehefrau) ist der Drogenkrieg ja nicht vorbei…

Emotet

Infrastruktur von Emotet abgeschaltet

Strafverfolger stoppen die gefährlichste Schadsoftware der Welt

Deutschen Ermittlern ist zusammen mit internationalen Partnern ein spektakulärer Schlag gegen die Betreiber der berüchtigten Schadsoftware Emotet gelungen. Ob der Erfolg von Dauer ist, muss sich aber erst zeigen.

Von **Patrick Beuth**
27.01.2021, 17.29 Uhr

…hat viele Versäumnisse und Missstände aufgezeigt

Emotet

Modulares Schadprogramm

Trickbot, …

Ryuk, …

Auch nach Emotet…

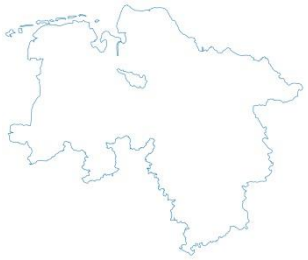
28.05.2021:	Verschlüsselung der Systeme inkl. Backup
31.05.2021:	Bereitschaft zu zahlen

Aussage des CEO: „Wir hatten keinen Notfallplan“

Auch nach Emotet…

Nachts 13. auf 14. März 2021:	Verschlüsselung der Systeme
Morgens am 15.03.2021	Verschlüsselung wird entdeckt
15.03.2021	Lösegeldforderung 56 BTC (ca. 1,7 Mio €)
16.03.2021	verhandelt auf 27 BTC (ca. 800 t €)
17.03.2021	Zahlung erfolgt
Anfang April 2021	Systeme wiederhergestellt

Problem 1: Supply chain… „compromise-one-compromise-many“
Problem 2: Double Extorsion



APT

Lapsus$ Conti

Wiper

Viasat/Ka-Sat Ghostwriter

…oder einfach der gelangweilte Jugendliche aus Mittelhessen…

Di|gi|ta|li|sie|rung

[ˌdigitaliˈziːʁʊŋ]

Industrie 4.0

IoT

digitale Gesellschaft

…das Problem dabei:

#WirhängenallesinsInternetwasnichtbeidreiaufdenBäumenist

#DafüristdasInternetnichtgeschaffenundauchnichtgeeignet

#Möglichkeitensindsexy_Risikennicht!

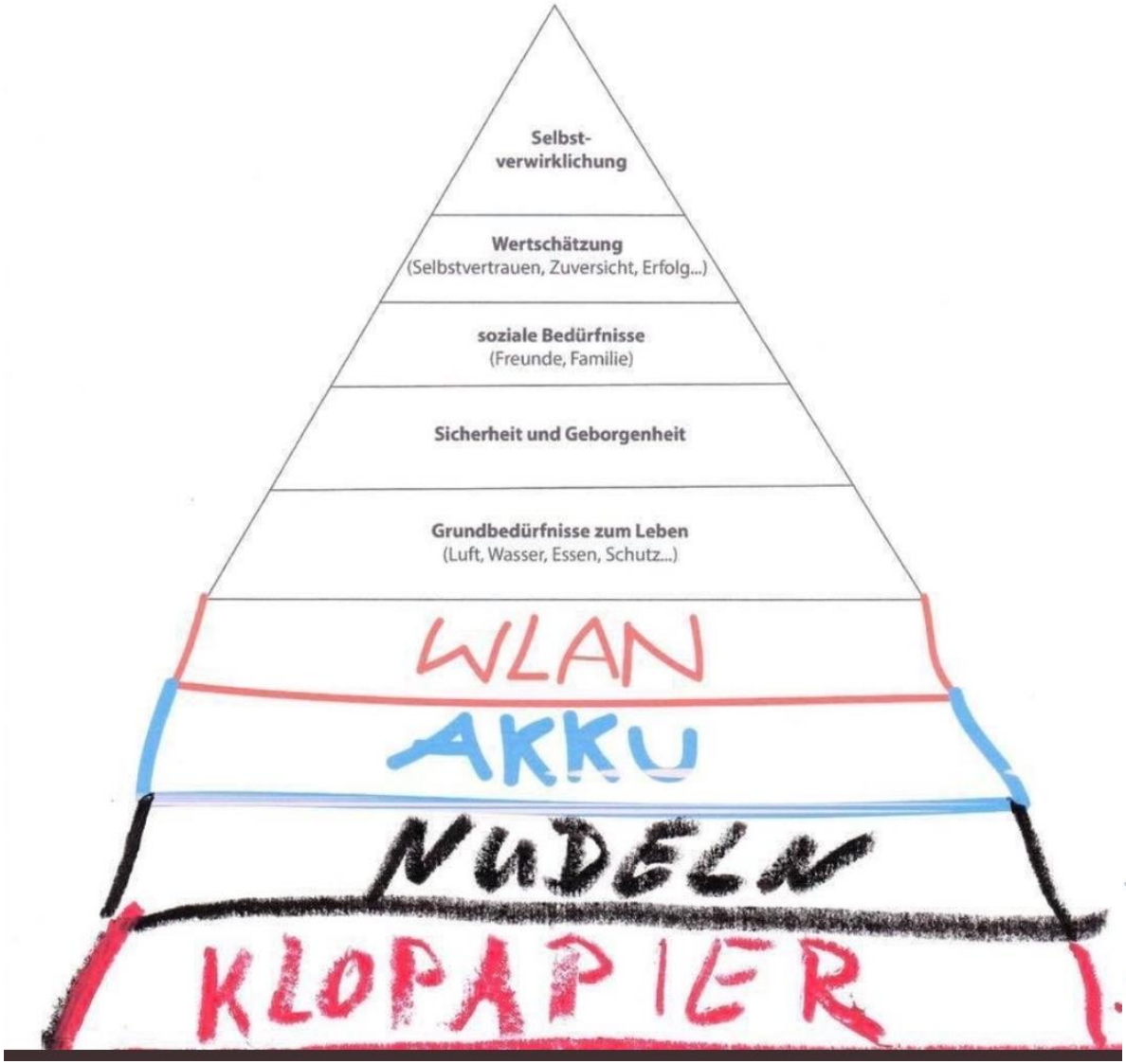
„The good news is that we are connected to the Internet.
The bad news is that the Internet is also connected to us.“

Grundbedürfnisse des Menschen

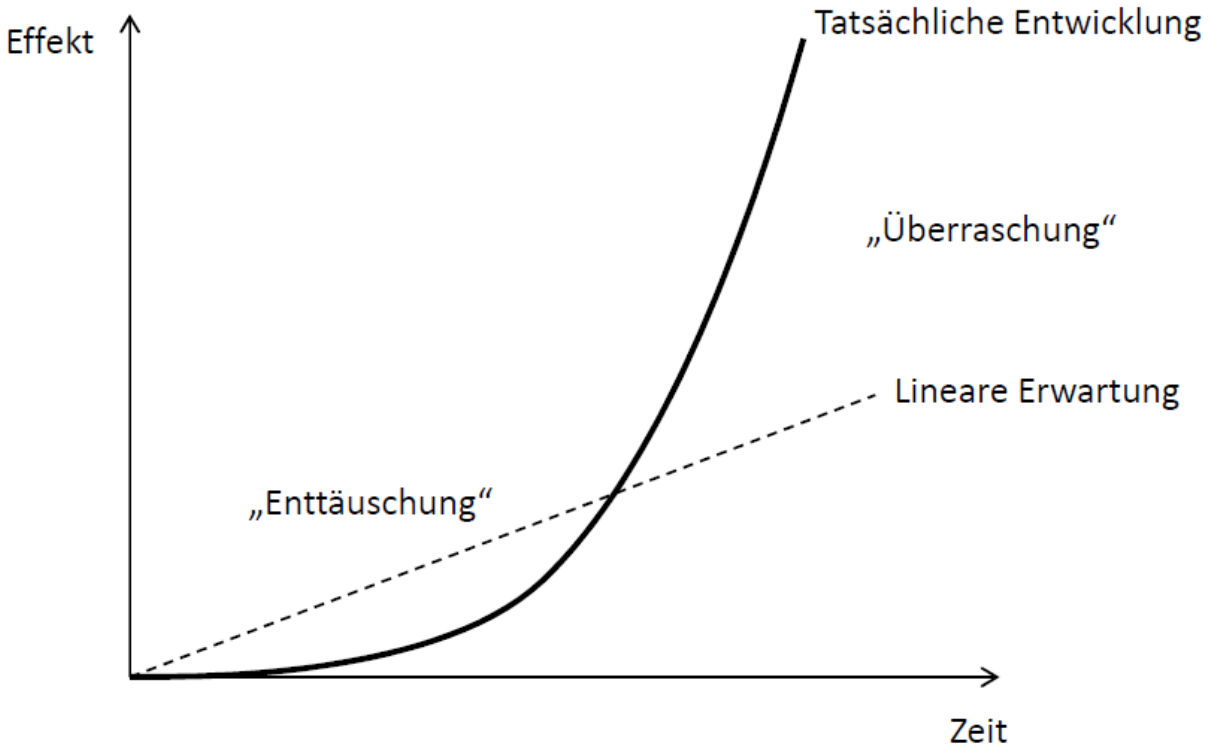
Mittelstand trifft Mittelstand, 12.05.2022
Risiken in einer vernetzten Welt

Grundbedürfnisse des Menschen

Mittelstand trifft Mittelstand, 12.05.2022
Risiken in einer vernetzten Welt



Menschen schätzen exponentielle Trends oftmals falsch ein

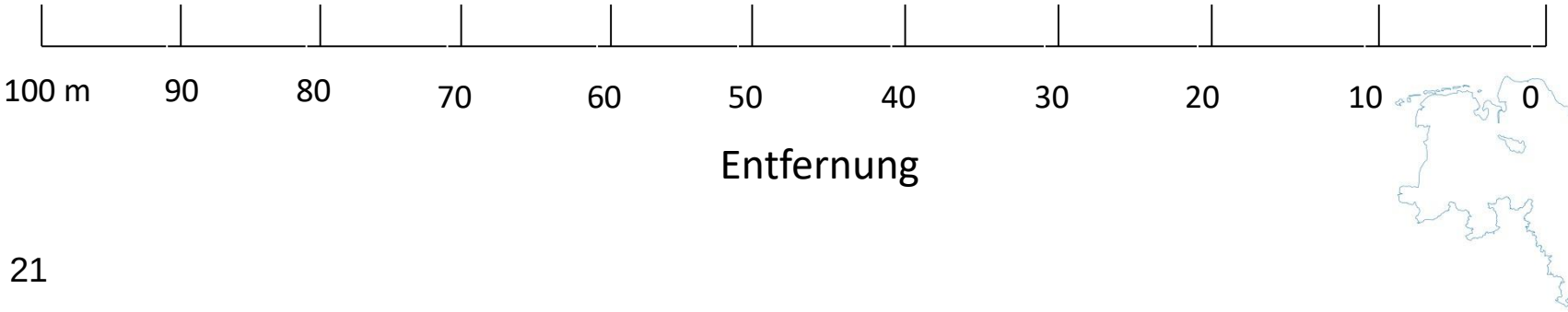


Mittelstand trifft Mittelstand, 12.05.2022
Risiken in einer vernetzten Welt

Das menschliche Gehirn ist auf lineares Denken ausgerichtet

linear

exponentiell



Die meisten Fehler werden immer noch von Menschen gemacht

…no patch for human stupidity…

Die meisten Fehler werden immer noch von Menschen gemacht

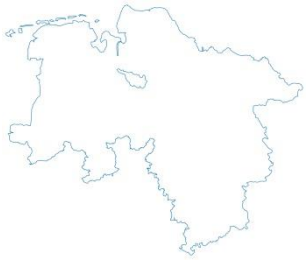
…no patch for human stupidity…

“If you think **technology** can solve your security **problems**, then you don't understand the **problems** and you don't understand the **technology**.”

“People often represent the **weakest link** in the security chain and are chronically **responsible for the failure of security systems**.”

Bruce Schneier

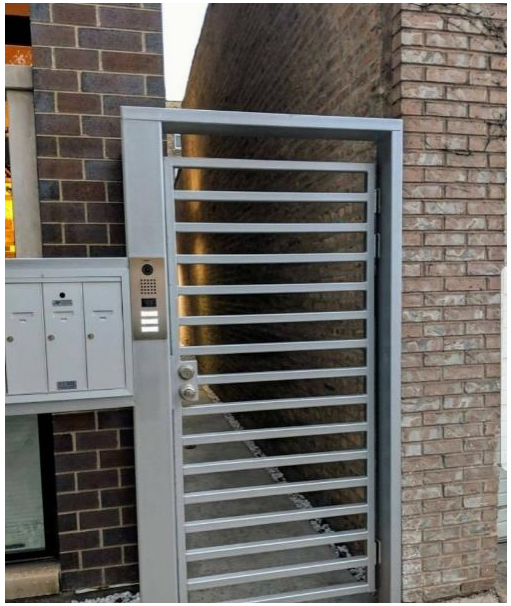
Sicherheit?



Mittelstand trifft Mittelstand, 12.05.2022
Risiken in einer vernetzten Welt

Gefahr

Schutz



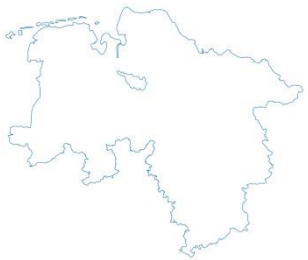
Risikobetrachtung

↓

Maßnahmenauswahl

↓

Umsetzung



Vorbereitung auf mögliche Schadensereignisse

Viel wichtiger als die Kenntnis aller Angriffsmöglichkeiten ist die Kenntnis der eigenen Verwundbarkeit, internen Strukturen und Prozesse

↓

Auf dieser Basis können konkrete Sicherheitsmaßnahmen für Unternehmen etabliert werden

Vorbereitung auf mögliche Schadensereignisse

Irgendwann wird es Sie treffen

↓

Notfallplan

Vorbereitung auf mögliche Schadensereignisse

Reserverad bei wish bestellt

Fazit?

Fazit?

Niedersächsisches Ministerium
für Inneres und Sport
Verfassungsschutz

Vielen Dank für Ihre Aufmerksamkeit!

Markus Böger
Verfassungsschutz Niedersachsen
Wirtschaftsschutz
+49 511 6709-284
+49 172 4265468
markus.boeger@mi.niedersachsen.de