

@-yet GmbH
Wolfgang Straßer
Geschäftsführer
Dipl.-Kfm.

147. Forum Mittelstand Oktober 2011 IHK Bochum und VoBa Sprockhövel



- Warum Information- und IT- Security?
- Datenklau passiert überall, zu jeder Zeit und völlig unverhofft
- Wie geht das von statten?

Firmenportrait

- Juni 2002 gegründet
- heute 28 Mitarbeiter
- Sitz: Leichlingen/Rheinland
- IT-Strategie- und Technologieberatung
 - kein HW- oder SW-Vertrieb
- Beratungsschwerpunkte
 - IT-Risikomanagement
 - IT-Outsourcing
- Zielgruppe:
 - mittelständische und große Organisationen und Unternehmen

@-yet Geschäftsbereiche



IT RESULTING IM FOKUS

Agenda

- ✓ Bedrohungslage – real oder aufgebauscht?
- ✓ Risiko Organisation und Mensch
- ✓ Nutzung von Web 2.0
- ✓ Nutzung mobiler Endgeräte und Technologien
- ✓ Live Hacking
- ✓ Diskussion

IT und Risikomanagement

IT-Risikomanagement =

Der bewusste und gezielte Umgang mit den Risiken, die sich für Organisationen durch den Einsatz von IT ergeben können!

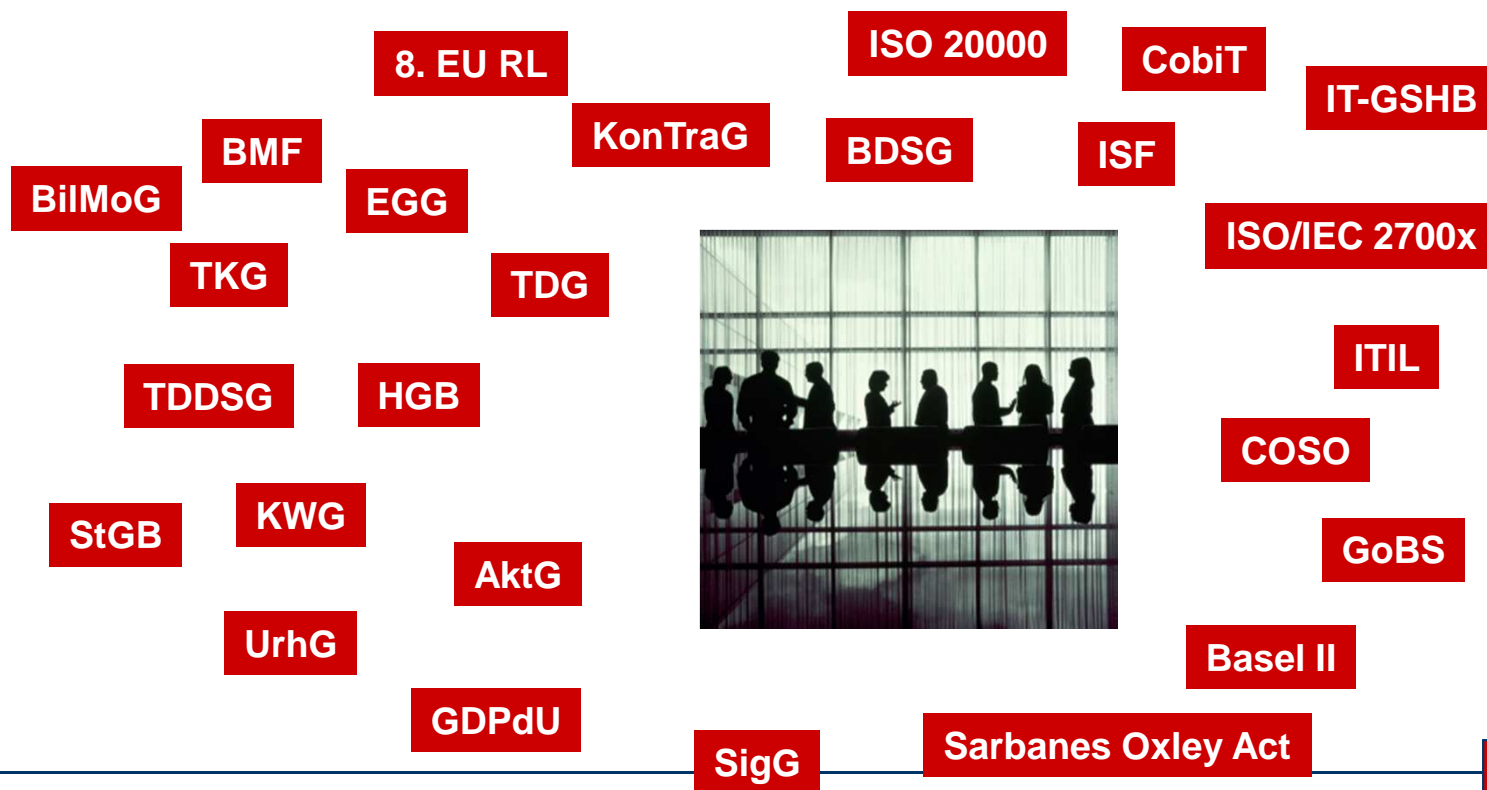
IT-Risikomanagement ist kein Selbstzweck

➤ Warum IT-Risikomanagement?

- Schutz vor Ausfällen/Stillständen
 - Produktion
 - Auslieferung etc.
- Schutz vor Know-how-Verlust
- Schutz vor dem Gesetzgeber
 - Compliance

Regulatorischer Dschungel

- der regulatorische Dschungel mit Bezug auf IT-Risikomanagement (Auszug):



➤ **IT- Security** ist

- nur ein Baustein eines ganzheitlichen, unternehmensweiten IT-Riskmanagements
- aber ein sehr wichtiger

IT Security

➤ Warum?

- ohne Einsatz von IT keine
 - Innovation
 - Produktion
 - Verkauf
 - Einkauf
 - einfach kein Geschäft mehr möglich

- in den Firmennetzen liegen
 - echte Assets
 - rechtliche Risiken!!

IT-Security

- Fakt ist
 - die Risiken nehmen zu
 - die Bedrohungslage ist wirklich ernst
 - es kann jeden treffen

- Oft gehört:
 - Wer interessiert sich für uns?
 - Antwort: der ganze Planet!

 - Bei uns ist noch nie was passiert!
 - Antwort: das wissen Sie gar nicht!

 - 100% Sicherheit gibt es nicht!
 - Antwort: stimmt, aber 10-20% sind aber definitiv zu wenig!

Business Security

➤ Motive der Angreifer

- wirtschaftliche
 - Wirtschaftsspionage
 - Konkurrenzausspähung
 - Erpressung
- Rache
- ethische Motive
- „Spaß am Hacken“
- viele mehr

Zahlen und Fakten

- ans Internet angeschlossene Rechner werden statistisch alle 39 Sekunden attackiert.
Im Durchschnitt 2244 Mal am Tag.
(Quelle: Heise, Studie der Universität Maryland)
- alle 14 Sekunden werden neue virenverseuchte Webseiten entdeckt, d. h. 6.000 pro Tag.
(Quelle: Sophos)
- Russisches Unternehmen zahlt 5 Millionen € p.a. an Vertreiber von vorgeblicher AV-Software, die PC entert.
(Quelle: New York Times)

Zahlen und Fakten

- US-Bericht: China verstärkt Spionageangriffe auf Unternehmen
 - geschätzter Verlust ca. 50 Mrd. US-Dollar (Quelle: Heise vom 23. Oktober 2009)
- Know-how Verlust in Deutschland ca. 20 Mrd. €/Jahr
 - (Quelle: Studie Universität Lüneburg)
- Alle 53 Sekunden wird in den USA ein Laptop gestohlen – 97 % bleiben für immer verschwunden
 - (Quelle FBI / Zeitung US Today)

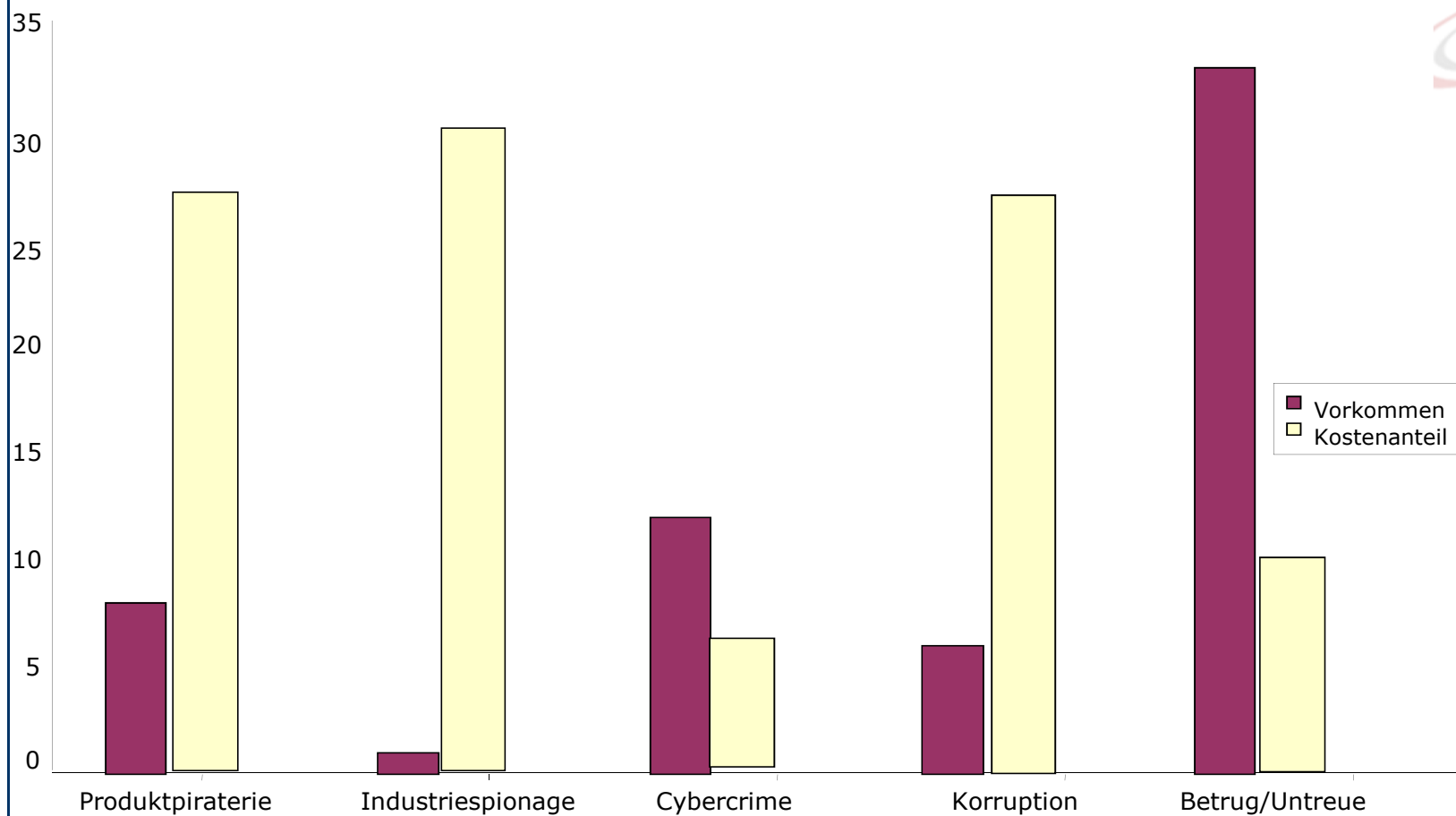
Zahlen und Fakten

➤ Wer ist betroffen?

- 57,6 % der mittelständischen Unternehmen
- 38,5 % der kleineren Unternehmen
- 3,9 % der Konzerne

- Bei 35,1 % der Unternehmen in NRW besteht Verdacht auf Spionage (Quelle: Corporate Trust)
 - **Eigeneinschätzung!!!!**

Schadensanteil Spionage



Quelle: PWC, Wirtschaftskriminalität 2003

Business Security

➤ Wer greift an?

- Geheimdienste
- Wettbewerber
- Besserwisser
- Weltverbesserer
- Scriptkiddies
- „Zufallstreffer“

=> Jeder der im Internet ist, kann!!!!!!

Business Security

- Was wird abgegriffen?
 - Unternehmens Know-how
 - Produktneuentwicklungen
 - Einkaufsinformationen
 - M&A Informationen
 - Kontendaten
 - Kundendaten
 - Unternehmensstrategie
 - etc.

Business Security

- Wie wird angegriffen?
 - Informationsbeschaffung von innen
 - klassisch
 - Erpressung
 - Jobwechsel
 - etc.
 - immer mehr
 - Wikileaks, der durfte das!!
 - SocialMedia/SocialEngineering

Business Security

➤ Wie läuft ein Angriff ab?

- Vorbereitung
 - Google Earth
 - Streetview
 - Socialnetworks
 - Phishing
 - Vor-Ort Analyse wird einfacher und unbemerkter vorbereitet
- Durchführung
 - Anrufe
 - Kontaktaufnahme via Socialnetwork
 - Zutritt zu Gebäuden
 - Installation von IT-Equipment

Business Security

➤ Wie läuft ein Angriff ab?

- Netzwerkscans
 - Was ist über das Unternehmen im Netz zu finden?
 - Wer ist der Provider?
 - Gibt es ggfs. bekannte IT-Lücken?
 - Wie ist der „Patch“zustand?
- Wie sieht die Website Security aus?
- Gibt es Online-Shops?
- Sammeln von Kennungen und Passwörtern via Phishing
- etc.

Social Networks, ein leichte Quelle

- detaillierte Informationen aus Social-Networks wie Facebook, StudiVZ oder Xing über:
 - Personen
 - Adressen
 - Hobbies
 - Kontakte/Freundschaften
 - Job / Rolle / Aufgabenbereich
 - Firmen/Behörden
 - Mitarbeiter
 - Firmengelände
 - Büro- und Behördenräume
 - Sicherheitsmaßnahmen

Beispiel Social Engineering I

Offizieller Zutritt als Besucher / Kunde

- Nutzung interner Ressourcen
- „Dumpster Diving“
- Diebstahl von materiellen und imm



enständen



Beispiel Social Engineering II

Inoffizieller Zutritt als z.B.
PC/TK Techniker

- Diebstahl von Daten auf USB-Stick



- Installation eines Keyloggers



- Installation eines Wireless-Access-P



- Sabotage von kritischen Systemen



Beispiel Social Engineering III

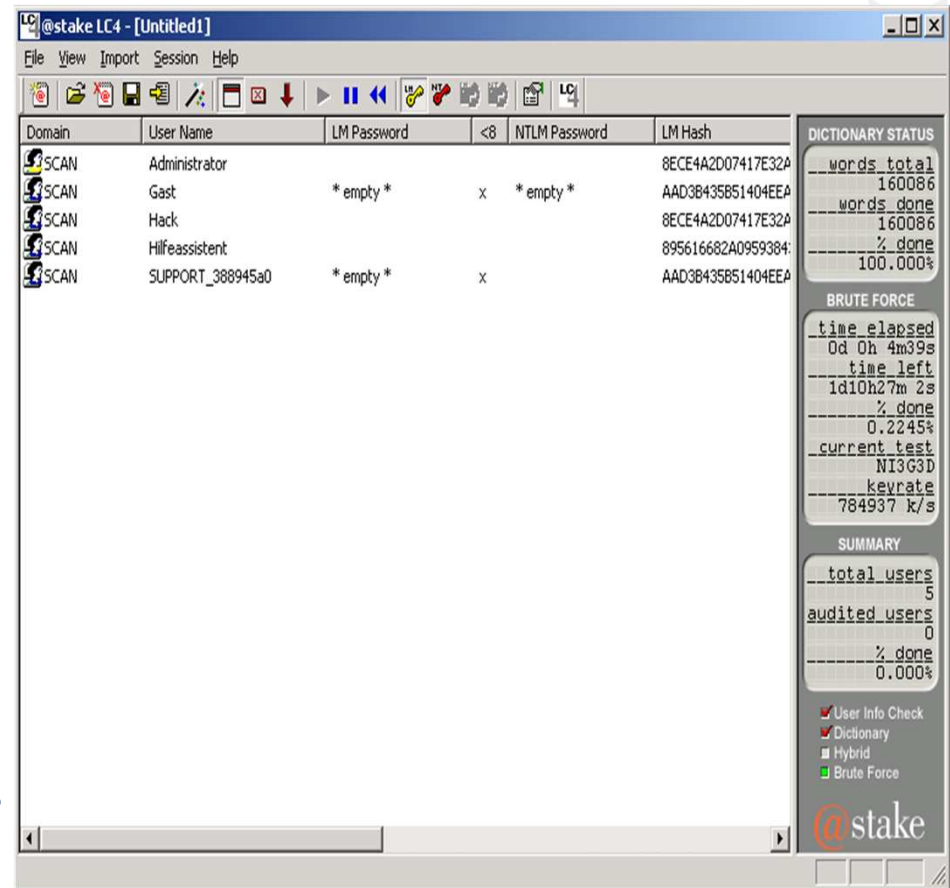
- außenstehende / Besucher können Gebäude & Räume „ungehindert“ betreten
- Firmeninterne Unterlagen einfach zugänglich
- Verteilerschränke sind nicht abgesperrt
- vertrauliche Daten in den Büros werden nicht weggesperrt bzw. Büros nicht abgeschlossen
- **Einschleusen von Trojanern via USB Sticks**



Beispiel: Password-Cracking

Systematisches Ausprobieren von Passwörtern mit Offline-Wörterbuch bzw. Brute Force

- Kopie der verschlüsselten Passwortdatei bzw. Ergebnis von Sniffing
- Verschlüsseln gebräuchlicher Worte und Vergleich mit den Einträgen in der Passwortdatei (z.B. mit dem frei erhältlichen Programm Crack)
- Bei Übereinstimmung des verschlüsselten Ergebnisses ist der Account des Benutzers für den Angreifer offen



Domain	User Name	LM Password	<8	NTLM Password	LM Hash
SCAN	Administrator				8ECE4A2D07417E32A
SCAN	Gast	* empty *	x	* empty *	AAD3B435B51404EEA
SCAN	Hack				8ECE4A2D07417E32A
SCAN	Hilfeassistent				895616682A0959384
SCAN	SUPPORT_388945a0	* empty *	x		AAD3B435B51404EEA

DICTIONARY STATUS

words_total: 160086
words_done: 160086
% done: 100.000%

BRUTE FORCE

time_elapsed: 0d 0h 4m39s
time_left: 1d10h27m 2s
% done: 0.2245%
current_test: NI3G3D
keyrate: 784937 k/s

SUMMARY

total_users: 5
audited_users: 0
% done: 0.000%

User Info Check
 Dictionary
 Hybrid
 Brute Force

@stake

Beispiel: mobile Devices

- **Objekt:** Smartphone/Handy/Pad
- **Verbindung:** Bluetooth
- **Geschwindigkeit:** 786 KBps
- **Schutz:** PIN

- **Reichweite¹⁾:** ca 4 Km
- **Dauer:** 0 Minuten

- **Ziele:** Telefonieren
Versand von SMS

Ausspionieren von Daten
Handy als Wanze
Smartphone als Firmenzugang

1) Mit handelsüblichen Richtfunkantennen/Verstärkern



Smartphones

- Sind überwiegend – derzeit - nicht sicher einbindbar ins Firmennetz
 - kaum zentral managebar
 - nur die wenigsten sind verschlüsselbar
 - enthalten oft viele Firmeninformationen
 - Emails
 - Kontakte
 - Kalendereinträge
 - **Systemzugangsdaten**
 - **VPN**
 - **Passwörter**
 - **Useraccounts!!**

Smartphones

- Sind überwiegend – derzeit - nicht sicher einbindbar ins Firmennetz
 - unsaubere Apps als Einfalltor
 - Trojaner
 - Viren
 - Erstellen „saubere“ Bewegungsdaten und melden diese online weiter
 - technisch leicht übernehmbar mittels
 - unsichere Bluetoothstacks
 - WLAN
 - SMS - Trojanereinschleusung

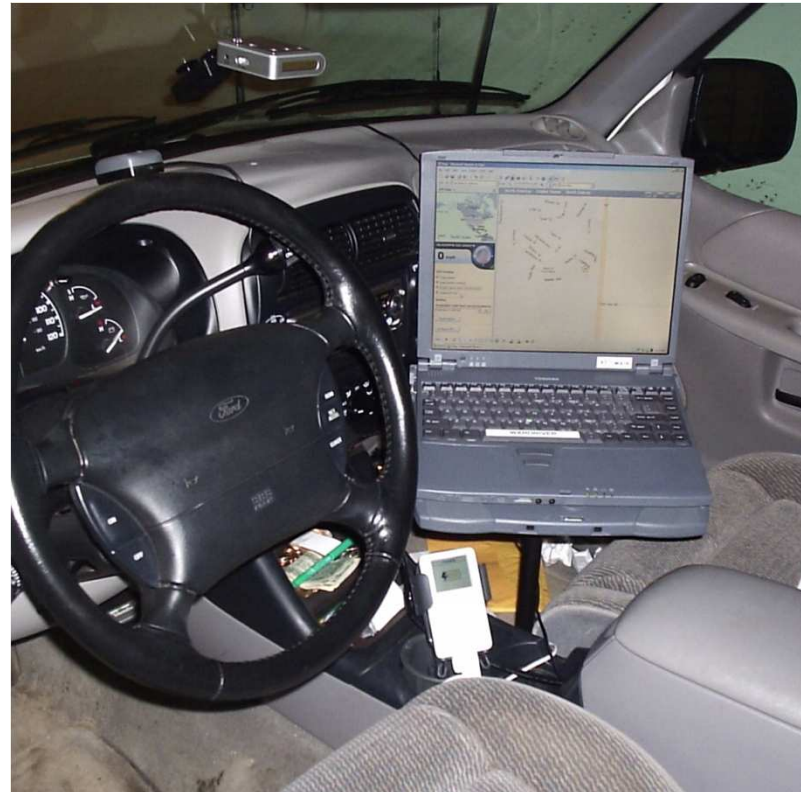
Beispiel: Wireless LAN/Hotspots

Objekt: Netzwerk/WLAN

- Verbindung: WLAN
- Geschwindigkeit: 54MBps
- Verschlüsselung: WEP
- Keystärke: 128 Bit

- Reichweite¹⁾: ca 5 Km
- Dauer: ca 3-7 Minuten

- Ziele: Zugang internes Netz
Internet Zugang
Ausspionieren von Daten
Angriff auf Fremdnetze
Blockieren von Zugriffen



1) Mit handelsüblichen Richtfunkantennen/Verstärkern

Cloud

- Merkmale der Cloud
 - große Anbieter haben RZ in der ganzen Welt
 - diese sind untereinander vernetzt
 - in bestimmten Ländern sind hochwertige Verschlüsselungsalgorithmen nicht zugelassen

 - Damit wird die Datensicherheit stark eingeschränkt bis unmöglich
 - auch Regionalisierung hilft da nicht, da RZ´s grundsätzlich vernetzt sind
 - echte Individualisierung nimmt den Kostenvorteil

 - Rechtliche Restriktionen
 - BDSG und Finanzbehörden

Vorgehensweise zum Schutz

- Bestimmen Sie ihren Schutzbedarf
 - Welche Daten sind für Ihr Unternehmen wie wichtig?
 - Datenklassifikation, ISMS
 - Welche Daten gehören in den Know-How Bereich?
 - Wer darf auf welche Daten zugreifen und darf er das?
 - 1. Welche Prozesse sind wie wichtig?
 - Business Impact Analyse
 - Welche gesetzlichen Mindestauflagen müssen Sie erfüllen?

Vorgehensweise zum Schutz

➤ Statusfeststellung: wo stehen Sie?

- Status organisatorische Sicherheit
 - Policies
 - Awareness
 - @-yet tools:
 - Social Engineering/Phishing
 - Policy Check
- 1. Status physische Sicherheit
 - Gebäudeschutz
 - @-yet tool:
 - Social Engineering
- Status IT Sicherheit
 - @-yet tools
 - Onsite- und Offsite-Pentests
 - Infrastruktur- und Continuitycheck

Was wollten wir Ihnen vermitteln

- Security zu vernachlässigen
 - ist fahrlässig
 - kann existentiell werden

- vor der Implementierung von Schutzmechanismen und -maßnahmen kommen die **Sicherheitsziele**

- die Technik ist komplex,
 - aber beherrschbar
 - ohne Organisation und Awareness ist sie wertlos

Was wollten wir Ihnen vermitteln...

➤ Organisatorische Sicherheit und Sicherheitsbewusstsein aller Beteiligten sind die kritischen Elemente von Know-How Schutz und Business Security!

und

➤ oben fängt es an - Chefsache

Appell

- ✓ 100% Sicherheit gibt es nicht
 - stimmt, das ist aber kein Grund
 - sich mit 10 oder 20 % Sicherheit zu begnügen
 - oder gar zu resignieren

Vielen Dank für Ihre
Aufmerksamkeit!

Ihre Fragen bitte ...



Wolfgang Straßer
wolfgang.strasser@add-yet.de