Wirtschaftsspionage

Risiken in einer vernetzten Welt

Wirtschaftsspionage
Risiken in einer vernetzten Welt
Geschäftsgeheimnis
Vertraulichkeit
Cybercrime
Risikomanagement
Sicherheitsstrategie
normal
hoch
Werkzeuge
IT-Grundschutz
Modellierung
DLP
Bring your own device
Geräte
Mobile Device Management
Schutzbedarfskategorien
ISMS
Schutzbedarf
Verantwortung
Integrität
Joint Venture
Notfallmanagement
Standard-Sicherheitsmaßnahmen
Überprüfung
Sicherheitsmanagement
Umsetzung
Schutzbedarfsfeststellung
Security
Sicherheitsziele
Audits
Innentäter
Kontrollmechanismen
Konzept
Verfügbarkeit
Netze
ISO 27001 / ISO 27002
Geschäftsprozesse
Maßnahmen
Leitfaden
Strukturanalyse
Räume
sehr hoch

When I hear cyber
I just wannacry

Niedersächsisches Ministerium
für Inneres und Sport

- Verfassungsschutz -

20. Symposium, Deutsche Gesellschaft
für Wehrtechnik e.V. 27.06.2018

Wer wir sind

Was wir machen

Der älteste überlieferte Spionagefall:

„Sende Männer aus, die das Land Kanaan erkunden…“

~ 1300 v. Chr. *4. Mose 13,1*

Die größte Schwachstelle in IT-Sicherheitssystemen:

Der Mensch

Die größte Schwachstelle in IT-Sicherheitssystemen:

Der Mensch / Layer 8

Es gibt keine technische Lösung für ein menschliches Problem

…no patch for human stupidity…

IT-Sicherheit?

Social Engineering

PW

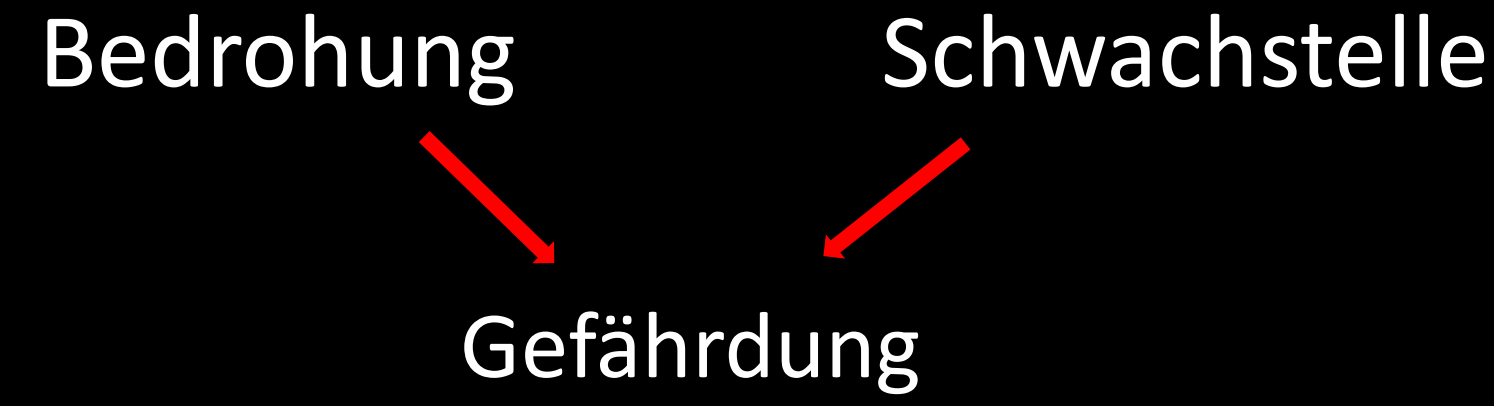
Problem: CEO-Fraud

Wirtschaftsspionage

betroffen?

Wirtschaftsspionage

gefährdet?


Bedrohung
Schwachstelle
Gefährdung

ca. 10.000 öffentlich bekannt gewordene Software-Sicherheitslücken pro Jahr

100+ Hackerangriffe pro Minute
200.000+ Schadcodes pro Tag

Tendenz steigend 

www.zone-h.com

It started with a „klick“

Beispiel: Ransomware

When I hear cyber
I just wannacry

Cryptowall:	18 Mio $
Locky:	17,3 Mio $
Cryptolocker:	3 Mio $
WannyCry:	80 t $
Wachstumsrate	2.500 %
Marktplätze	6.300+
Produkte	45.000+
Ø-Preis	10 $

Cryptowall: 18 Mio $

Locky: 17,3 Mio $

Cryptolocker: 3

WannyCry: 80

Grund 2:

Es ist lukrativ!

Wachstum: 2.500 %

Markt: 6.300+

Produkte: 45.000+

Ø-Preis: 10 $

Exploit-Kits / Malware-Baukästen

RIG, Sundown, Nebula,
Terror Exploit Kit, …

ca. 136.000 Nutzer

ca. 4 Mio. Angriffe in 04/2018

Takedown in 05/2018

Date Added	D	A	V	Title	Platform	Author
2018-04-06		-		LineageOS 14.1 Blueborne - Remote Code Execution	Android	Marcin...
2018-03-30		-		Advantech WebAccess < 8.1 - webvrpcs DrawSrv.dll Path BwBuildPath Stack-Based Buffer...	Windows	Chris Lyne
2018-03-29		-		Exodus Wallet (ElectronJS Framework) - Remote Code Execution (Metasploit)	Windows	Metasploit
2018-03-29		-		GitStack - Unsanitized Argument Remote Code Execution (Metasploit)	Windows	Metasploit
2018-03-28		-		TestLink Open Source Test Management < 1.9.16 - Remote Code Execution (PoC)	Linux	Manish Tanwar
2018-03-26		-		Acrolinx Server < 5.2.5 - Directory Traversal	Windows	Berk Dusunur
2018-03-16		-		Unitrends UEB 10.0 - Unauthenticated Root Remote Code Execution	Linux	Jared Arave

Web Application Exploits

This exploit category includes exploits for web applications.

Date Added	D	A	V	Title	Platform	Author
2018-04-13		-		**Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution**	**PHP**	**Hans Topo**
2018-04-13		-		**Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)**	**PHP**	**Vitalii Rudnykh**
2018-04-12		-		**Joomla Convert Forms version 2.0.3 - Formula Injection (CSV Injection)**	**PHP**	**Sairam Jetty**
2018-04-10		-		WordPress Plugin File Upload 4.3.3 - Stored Cross-Site Scripting (PoC)	PHP	ManhNho
2018-04-10		-		WordPress Plugin File Upload 4.3.2 - Stored Cross-Site Scripting	PHP	ManhNho
2018-04-10		-		Dell EMC Avamar and Integrated Data Protection Appliance Installation Manager - Invalid...	Linux	SlidingWindow
2018-04-10		-		WUZHI CMS 4.1.0 - Cross-Site Request Forgery (Add User)	PHP	taoge

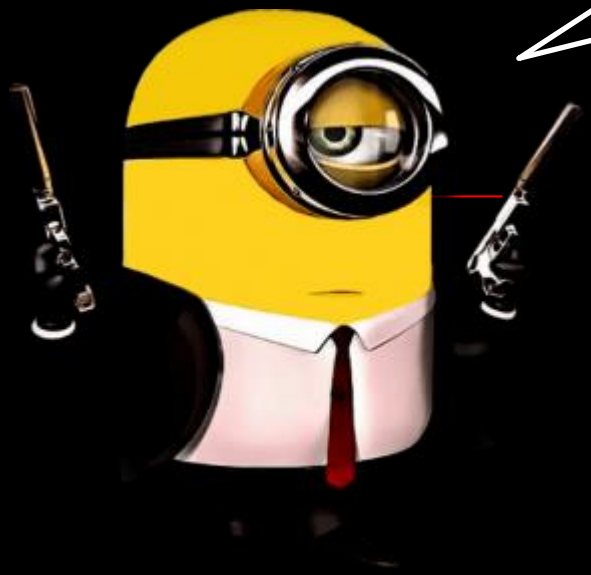
Local & Privilege Escalation Exploits

This exploit category includes local exploits or privilege escalation exploits.

Date Added	D	A	V	Title	Platform	Author
2018-04-10		-		DVD X Player Standard 5.5.3.9 - Buffer Overflow	Windows_x86	Prasenjit...

Grund 3:

Ohne großes Know-how!



Crime as a service

„There are only two types of companies, those that have been hacked and those that will be.“

Robert Mueller, Head of FBI

Immer wenn jemand an seinem PC auf „Eigene Dateien“ drückt, fällt irgendwo ein NSA-Mitarbeiter lachend vom Stuhl

(russische) Cyberangriffskampagnen

- Technische, finanzielle, … Anforderungen

- Interessen: Energie, Sicherheit, Außenpolitik, Militär, …

- Ziele: Regierungen, Politiker, Wirtschafts- und Forschungsunternehmen, …

- APT 28 (Fancy Bear, …)
- APT 29 (Cozy Bear, …)
- Snake (Turla, Uroburos, …)
- Berserk Bear (Energetic Bear, Dragenfly, …)
- […]

- Sachverhalt
- Handlungsempfehlung
- Vorbeugende Maßnahmen
- Netzwerkbasierte IOCs
- Hostbasierte IOCs

Digitalisierung

Digitale Transformation

Industrie 4.0

IoT

digitale Gesellschaft

Problem:

#WirhängenallesinsInternetwasnichtbeidreiaufdenBäumenist

#DafüristdasInternetnichtgeschaffenundauchnichtgeeignet

#Möglichkeitensindsexy_Risikennicht!

„Wir bauen unsere digitale Welt auf ganz schön viel Schrott“

Constanze Kurz, CCC, Handelsblatt 02.01.2018

Die Chancen der Digitalisierung nutzen

und die Risiken der Digitalisierung kennen

„The good news ist that we are connected to the Internet.

The bad news is that the Internet is also connected to us.“

Problem: Erkennen der Betroffenheit

Vielfältigkeit der Angriffe

Sie müssen sich vor ALLEN Schwachstellen schützen

–

Angreifer benötigen aber nur EINE Schwachstelle

Fazit?

Sicherheit – kostet Geld
Schaden – kostet die Existenz

Fazit?

Kein Backup?
Kein Mitleid!

Fazit?

Ganzheitliche Betrachtung von Sicherheit

Markus Böger, Polizeihauptkommissar
Verfassungsschutz Niedersachsen
Ref. 55, Wirtschaftsschutz
Tel.: 0511 / 6709-284
Email: markus.boeger@verfassungsschutz.niedersachsen.de