Cyber Risiken – für KMU (k)ein Thema?

EXPERTsuisse, Sektion Bern

VORABENDVERANSTALTUNG

Bern 28. November 2017

Agenda

Cyber Risiken - Aktuelle Lage

Kenne deinen Feind!

Modus Operandi

Schutzmassnahmen

Ausblick

Unser Alltag.....

Switzerland suspects Russian involvement in cyber attacks

Friday, May 6, 2016 7:05:00 AM

The Ministry of Defense of Switzerland was attacked in January and Russia is likely behind it.

Cyber-Attacken

Kriminelle erpressen Schweizer Online-Shops

NZZ AM SONNTAG / von Marcel Metzler / 21.9.2016, 18:02 Uhr

Digitec hat nach Cyber-Attacken mittlerweile Lösegeld-Forderungen erhalten. Die Firma ist kein Einzelfall. Die Schweiz ist schlecht geschützt.

Hackerangriffe auf VBS und Ruag

Geschäftsprüfungsdelegation wollte Geheimhaltung aufheben

4.5.2016, 15:02 Uhr

Der Bund ist Ziel ausländischer Betriebsspione geworden. Das bestätigt Bundesrat Guy Parmelin. Offenbar wurden streng geheime Daten entwendet.

An F/A-18 Hornet fighter aircraft of the Swiss Air Force releases flares. File photo: AFP

Swiss military hit by series of cyber attacks

➡ **GLOBAL CYBER-ATTACK ALERT (MAR 14, 2016): CIA Plotting Real-World and/or Cyber Attack on CERN, Internet-Related Infrastructure and/or Electrical Power Grids to Take Down Internet in Switzerland**

Posted: March 14, 2016 in Breaking News

Cyber-Attacke gegen Rüstungskonzern Ruag

Russische Hacker enttarnen geheime Schweizer Elitetruppe

NZZ AM SONNTAG / von Stefan Hübler, Andreas Schmid / 8.5.2016, 08:12 Uhr

Mit dem Spionageangriff auf die Ruag sind auch die Personalien der Sondereinheit AAD 10 der Armee entwendet worden. Es wird geprüft, den Soldaten neue Identitäten zu verleihen.

DDoS attack that d
was largest of its k
experts say

Dyn, the victim of last week's denial
orchestrated using a weapon called t
source of malicious attack'

Major cyber attack disrupts interne

Cyber-attacks to a number of Swiss supermarkets

Websites belong to the Swiss largest supermarket chains Migros and Coop and the country's Federal Railways are mostly suffered... There were also attempts by the hackers to blackmail the targeted companies. These were so called denial-of-service (DDoS) attacks, which occur when multiple systems flood the bandwidth of a targeted system, usually one or more web servers. This kind of cyber-attacks is often the result of a botnet.

These attacks which paralyzed IT and telephone system is a network with software specifically designed to disrupt or damage computer systems.

Swiss companies have recently suffered their biggest ever coordinated cyber-attacks; Switzerland su particularly vulnerable to these attacks because of its high-tech infrastructure and financial services sector. Swiss companies faced huge losses from cyber-attacks, a report published in 2015 by the professional service company KPMG, stated that Swiss companies suffered losses of over CHF200 million ($206 million) due to cyber-crime in 2014.

In recent times, the emails of 6000 Swiss small companies and private individuals were also hijacked apart from large scale commerce.

....und bei den KMU's ?

Donnerstag, 02.03.2017 / 16:34

Hacker-Angriff: War geschädigte Berner Firma nachlässig?

Internet-Kriminelle haben rund 1,2 Millionen Franken von den Konten der Berner Firma Küng Holding abzweigen können. Bis auf 160'000 Franken ist das Geld zwar wieder zurück, doch der Ärger bei Firmenchef Christoph Küng ist gross.

Zum einen staunt er, dass drei Banken ohne Rückfrage die Zahlungen an obskure Adressen auslösten. Im einen Fall ging es um 785'000 Franken an eine Einzelperson in Kirgistan. Zum anderen nervt sich Küng über die Zahlungssoftware, die seiner Ansicht nach ein gravierendes Sicherheitsproblem aufweise.

Das habe die Zahlungsaufträge der Hacker erst ermöglicht, sagte Küng am Donnerstag der Nachrichtenagentur 'sda'. Er bestätigte Berichte von 'Inside Paradeplatz', 'Bund' und 'Berner Zeitung'. Die Internet-Kriminellen hatten mit dem Trojaner Gozi operiert, der sich über den Anhang in einem E-Mail in fremden Computern einnistet.

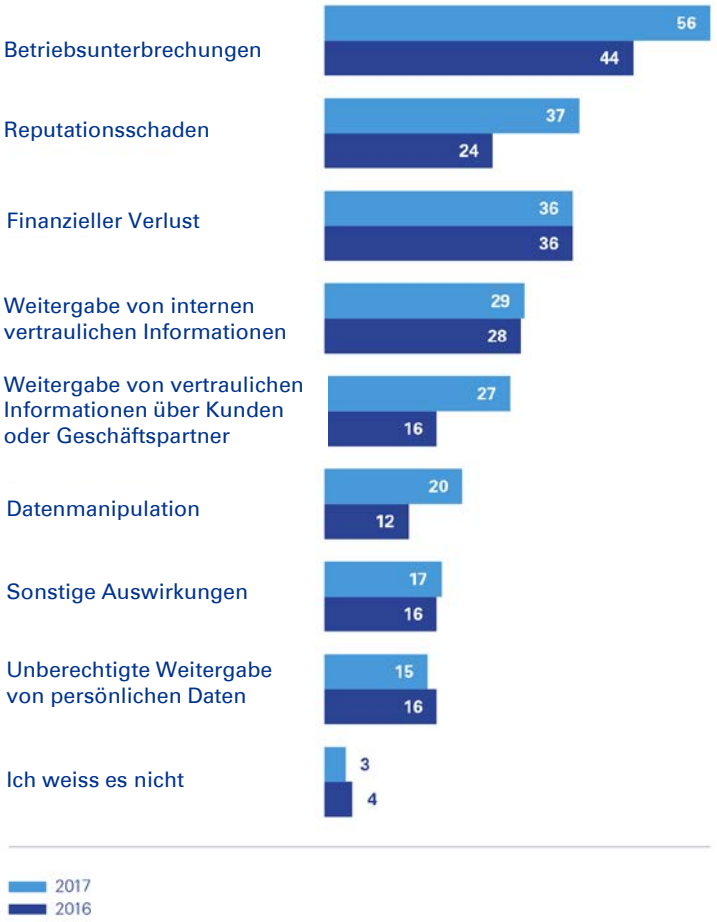
No need to cry if you keep your software up to date ?

Cyber-Angriffe nehmen zu

97% der Umfrageteilnehmer aus diversen KMUs haben in den letzten 12 Monaten eine Cyber-Attacke erlebt

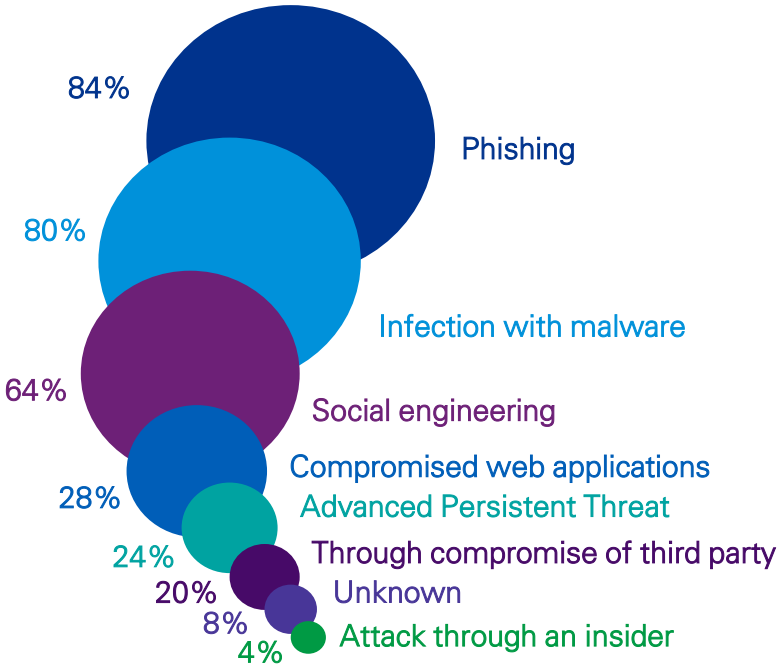
(Ergebnisse aus den Vorjahren:
2017: 88%
2016: 54%
2015: 52%)

Welche Auswirkungen auf Ihr Geschäft hatten die erfolgten Cyber-Attacken? (in Prozent)



Cyber Bedrohungen

Was war die Art des Angriffs welchen Sie in ihre Unternhemung festgestellt haben?



Source: KPMG Clarity on Cyber Security

Der Einfluss der Regulationen – ein Beispiel

EU General Data Protection Regulation (GDPR) adopted on April 14, 2016

HUGE FINES
Up to 20 million EUR or 4% of global annual turnover, whichever is higher

REAL REPUTATIONAL RISK
Breach notification within 72 hours

LARGE GEOGRAPHIC REACH
Applicable to **all organizations offering goods or services to EU citizens' and 'organizations** that monitor (online) behavior of EU citizens'.

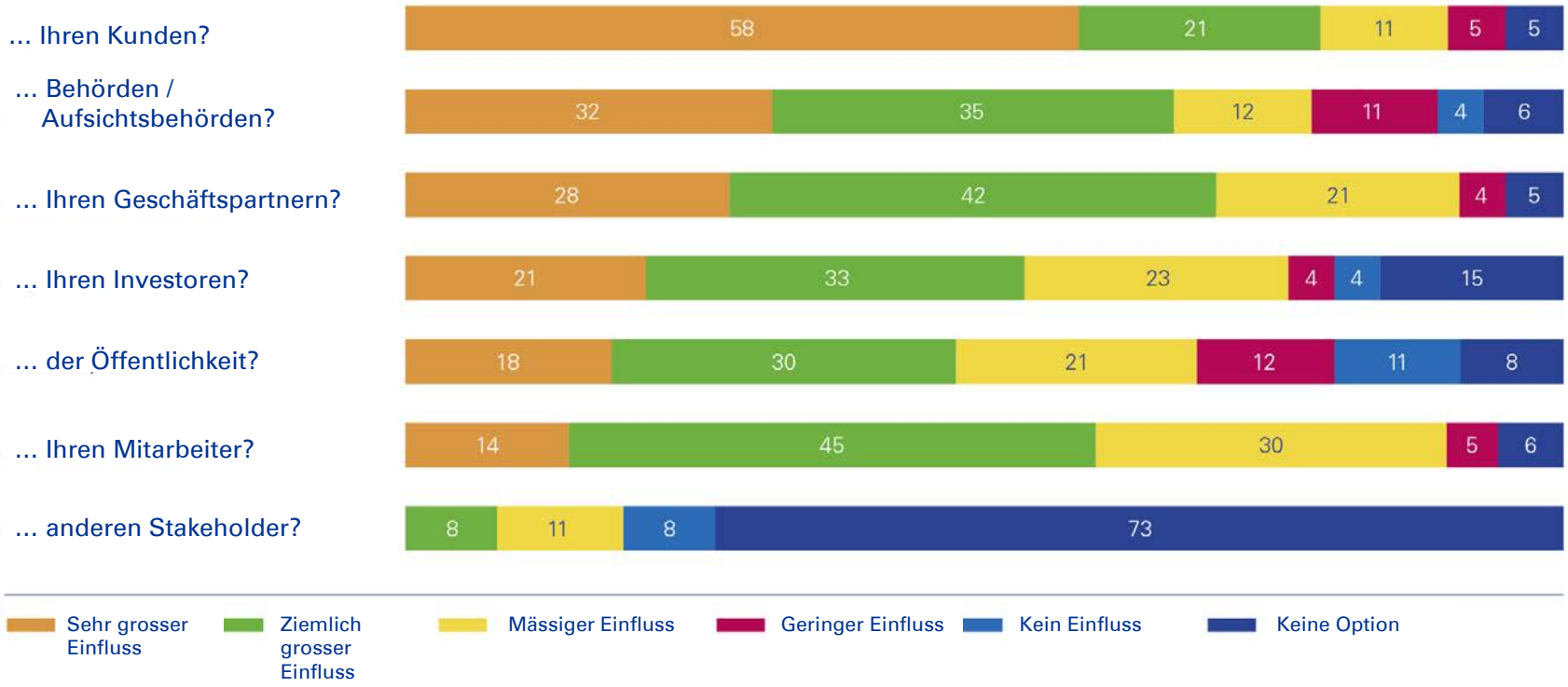
Swiss Data Protection Law currently under revision -will include similar clauses

Die menschliche Komponente von Cyber Sicherheit

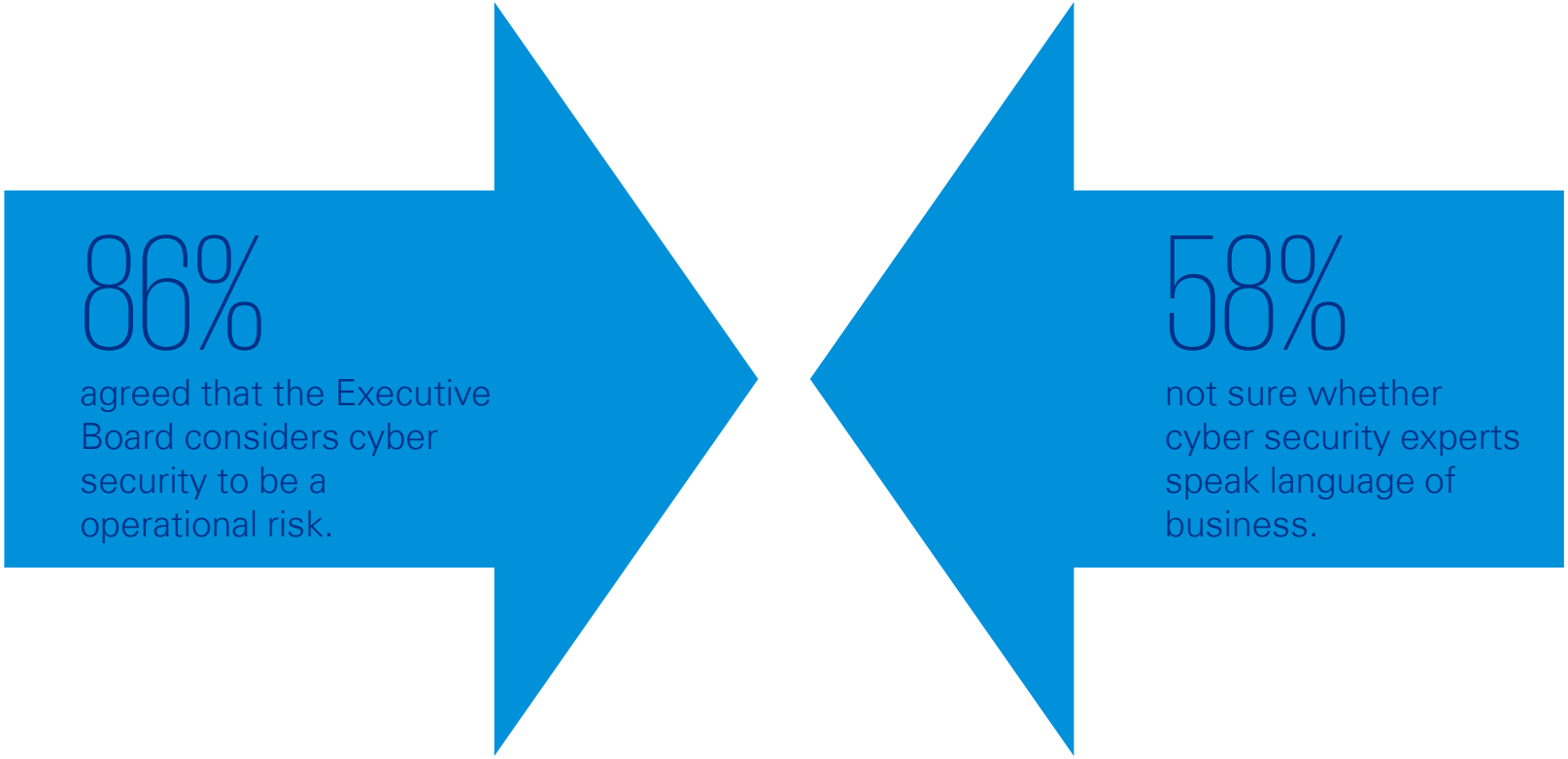
- Bei Sicherheit geht es ums Vertrauen
- Die menschliche Komponente war, bleibt und wird immer das schwächste Glied sein
- Es gibt ein Design-Problem – Benutzerfreundlichkeit der Sicherheitsmassnahmen wird nicht berücksichtigt

Cyber Security ist Vertrauen schaffen...

Inwieweit beeinflussen die Cyber-Sicherheit-Verletzungen das Vertrauen von... (in Prozent)



Cyber Risiken – Wahrnehmung ja - verstehen na ja...



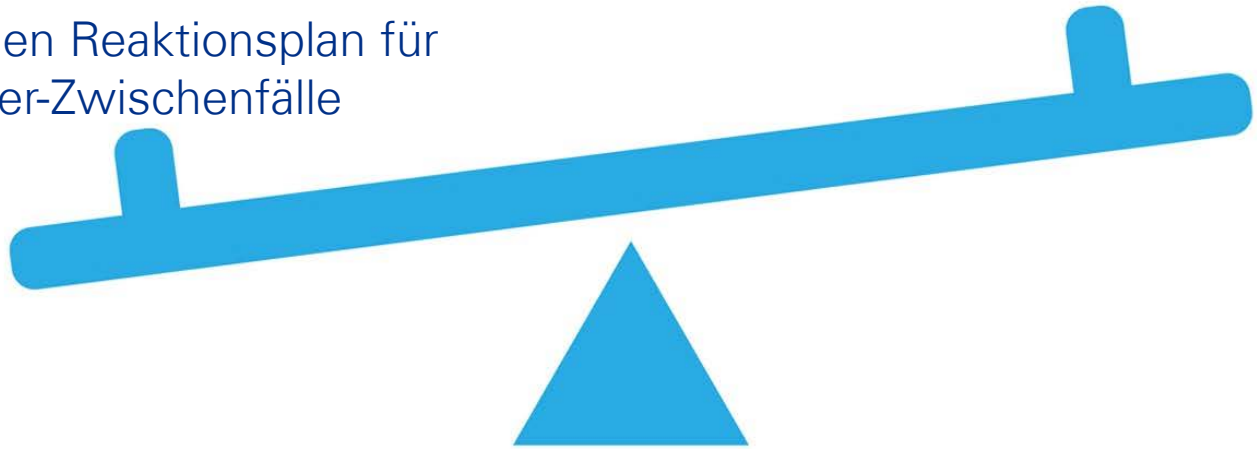
Unterschiedliche Geschwindigkeiten von Cyber Response

41%

der KMUs haben keinen Reaktionsplan für Cyber-Zwischenfälle

25%

der Grossunternehmen haben keinen Reaktionsplan für Cyber-Zwischenfälle



Kenne deinen Feind..!

Das Verständnis der Motivation, Absicht, Strategie, Taktik und die Mittel der Angreifer zu kennen, ist eine entscheidende Voraussetzung, um die Bedrohung zu antizipieren und effektive Massnahmen zur Verhinderung, Erkennung und Reaktion auf Angriffe vorzubereiten.

»Kenne deinen Feind und erkenne dich selbst«:
Zitat Philosophen Sun Tzu «Die Kunst des Krieges» (500 Jahre v.C.)

Täterprofile

80% der Befragten verfügen nicht über ein geeignetes Insider-Threat-Management-Programm.

HACKTIVISM

Ideologisch inspiriertes Hacking

ORGANISED CRIME

Global – schwierig aufzuspüren und zu verfolgen

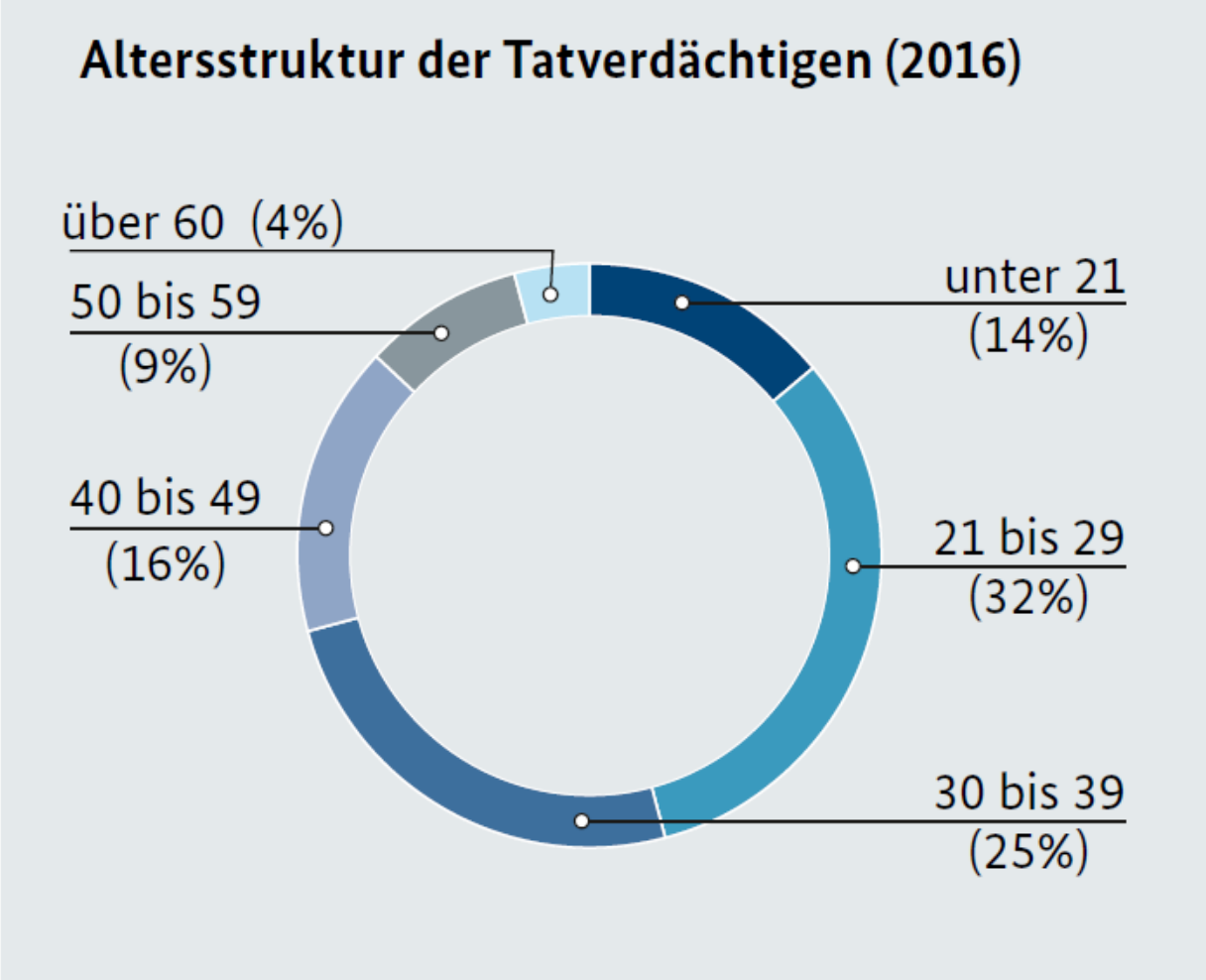
THE INSIDER

Vorsätzlich oder ungewollt?

STATE-SPONSORED

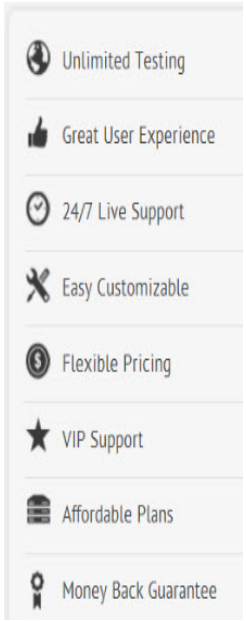
Spionage und Sabotage

Täterprofile



Quelle: Cybercrime Bundeslagebild 2016, Bundeskriminalamt, Wiesbaden

Kein Know-how erforderlich- Einkauf bei Darknet möglich



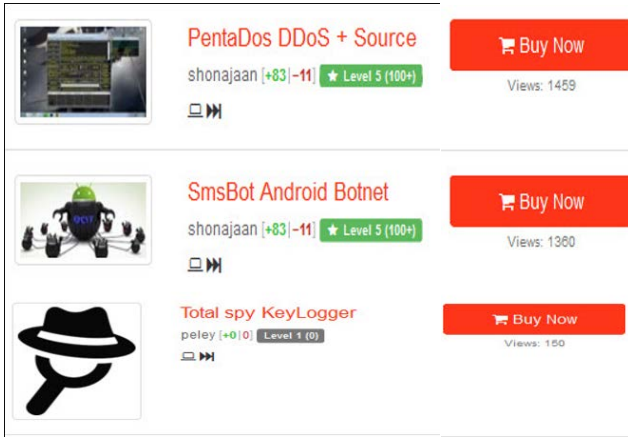
24 Hours DDoS Service

Vendor	antiman128 (10) (5.00⭐) (Ⓐ 8/0/1)
Price	฿0.935 (€510)
Ships to	Worldwide
Ships from	neterlands
Escrow	Yes

Product description

24 Hours DDoS Service, take out any target.

Terms and conditions of antiman128



Diamond Fox/Gorynych Botnet | Non-cracked

USD 370.00

฿ 0.6076

In stock

Shipping options

Express [Next Day] [+ USD 0.00]

Vendor	Mythoclast [+0|0] Level 1 (0)
Class	Digital

Gesetze - (Auszug)

Straftatbestand	Objektiver Tatbestand	Subjektiver Tatbestand	Täterprofil
Unbefugte Datenbeschaffung Art. 143 StGB	***Beschafft*** *sich gegen seinen* ***unbefugten Zugriff besonders geschützte*** *Daten, die einem* ***Anderen zustehen,*** *und die zu* ***verfügen*** *er* ***nicht berechtigt*** *ist.*	***Wissen****, dass die Daten einem andern zustehen und besonders geschützt sind.* ***Wille*** *bzw. Inkaufnehmen sich die Daten zu beschaffen.*	Externe Täter
Unbefugtes Eindringen in ein Datenverarbeitungs-system Art. 143 bis StGB	*Der Täter dringt ohne Berechtigung über eine Datenverbindung in eine gegen seinen Zugriff besonders geschützte, fremde Datenverarbeitungsanlage ein.*	***Vorsätzliches*** *Eindringen in eine fremde Daten-verarbeitungsanlage. Wer irrtümlich oder durch ein Versagen der Technik in eine fremde Datenverarbeitungs-anlage gelangt, ist nicht strafbar*	Externe Täter
Datenbeschädigung– Art. 144 bis StGB	*1) Der Täter* ***unbefugt elektronisch*** *oder in vergleichbarer Weise gespeicherte oder* ***übermittelte Daten verändert, löscht oder unbrauchbar macht****. Erforderlich ist eine Substanzveränderung.* *2) Wer* ***Programme****, von denen er weiss oder annehmen muss, dass sie zu den in* ***Ziffer 1 genannten Zwecken verwendet*** *werden sollen,* ***herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt****,*	*Vorsatz*	Externe Täter
Betrügerischer Missbrauch einer Datenverarbeitungs-anlage Art. 147 Abs.1 StGB	*Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt,*	*Vorsatz* *2) Handelt der Täter gewerbsmässig* *3) Der betrügerische Missbrauch einer Datenverarbeitungsanlage zum Nachteil eines Angehörigen oder Familiengenossen*	Externe Täter

Gesetze - (Auszug)

Straftatbestand	Objektiver Tatbestand	Subjektiver Tatbestand	Täterprofil
Wirtschaftlicher Nachrichtendienst Art. 273 StGB	***Auskundschaften*** *eines Fabrikations- oder Geschäftsgeheimnisses oder* ***zugänglichmachen*** *eines Fabrikations- oder Geschäftsgeheimnisses.*	*Auskundschaften erfordert die Absicht, das Geheimnis einem Adressaten zugänglich zu machen.*	Innentäter
Verletzung des Fabrikations- oder Geschäftsgeheimnisses Art. 162 StGB	*Zwei verschiedene Verhaltensweisen:* ***Verrat*** *eines Fabrikations- oder Geschäftsgeheimnis, infolge er in seiner* ***gesetzlichen oder vertraglichen Pflicht bewahren*** *sollte oder sich den* ***Verrat zu nutzen machen.***	***im Bewusstsein*** *seiner Geheimhaltungspflicht handeln.*	Innentäter
Tatbestand des Art. 47 BankG	*Pflichtwidrige Verletzung der ihm bekannten Geheimhaltungs- und Sorgfaltspflicht oder zu einer solchen* ***Verletzung*** *des Berufsgeheimnisses* ***verleitet.***	***wissentlich*** *ein Geheimnis offenbaren.*	Innentäter

Weitere:

- Verbotene Handlungen für einen fremden Staat – Art. 271 StGB
- Erpressung – Art. 156 StGB
- Verletzung von Fabrikations- und Geschäftsgeheimnissen – Art. 6 UWG
- Unbefugtes Verwerten von Informationen – Art. 50 FMG
- Straftat gegen den Geheim- oder Privatbereich
- Urheberrecht und verwandte Schutzrechte
- Datenschutzgesetz – DSG

Statisik- (Auszug)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

STAT-TAB – interaktive Tabellen (BFS)

Deutsch

>> px-x-1903020100_101 >> Polizeilich registrierte Straftaten gemäss Strafgesetzbuch nach Kanton, Ausführungsgrad und Aufklärungsgrad

Bearbeiten und berechnen | Speichern unter | Tabelle - Layout 2

xlsx CSV PX

Tabelleneinstellungen

Speichern Sie Ihren Datenauszug

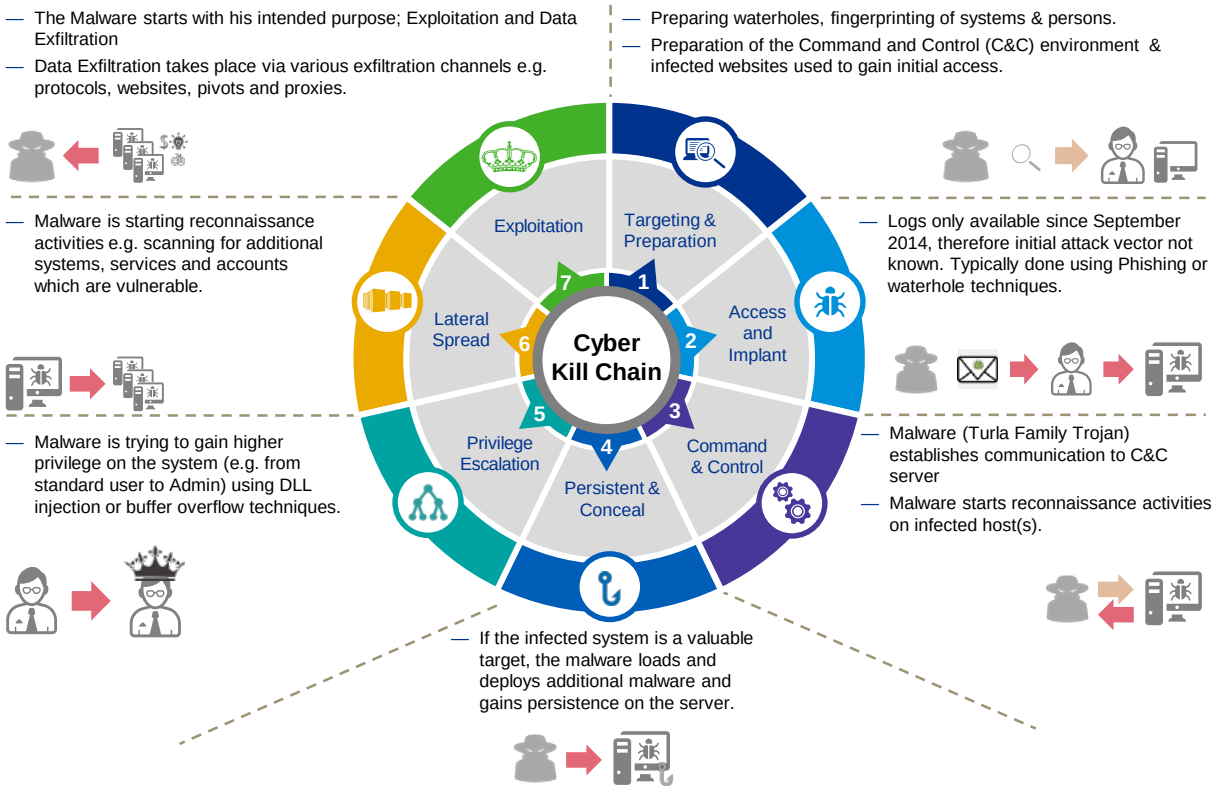
Polizeilich registrierte Straftaten gemäss Strafgesetzbuch nach Jahr, Kanton, Straftat, Ausführungsgrad und Aufklärungsgrad

			Vollendet		Versucht	
			Unaufgeklärt	Aufgeklärt	Unaufgeklärt	Aufgeklärt
2016	Schweiz	Unbefugte Datenbeschaffung (Art. 143)	762	190	19	8
		Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis)	259	112	10	2
		Datenbeschädigung, inkl. geringfügig (Art.144bis)	230	63	7	0
		Betrügerischer Missbrauch einer Datenverarbeitungsanlage, inkl. geringfügig (Art. 147)	2.964	1.218	434	172

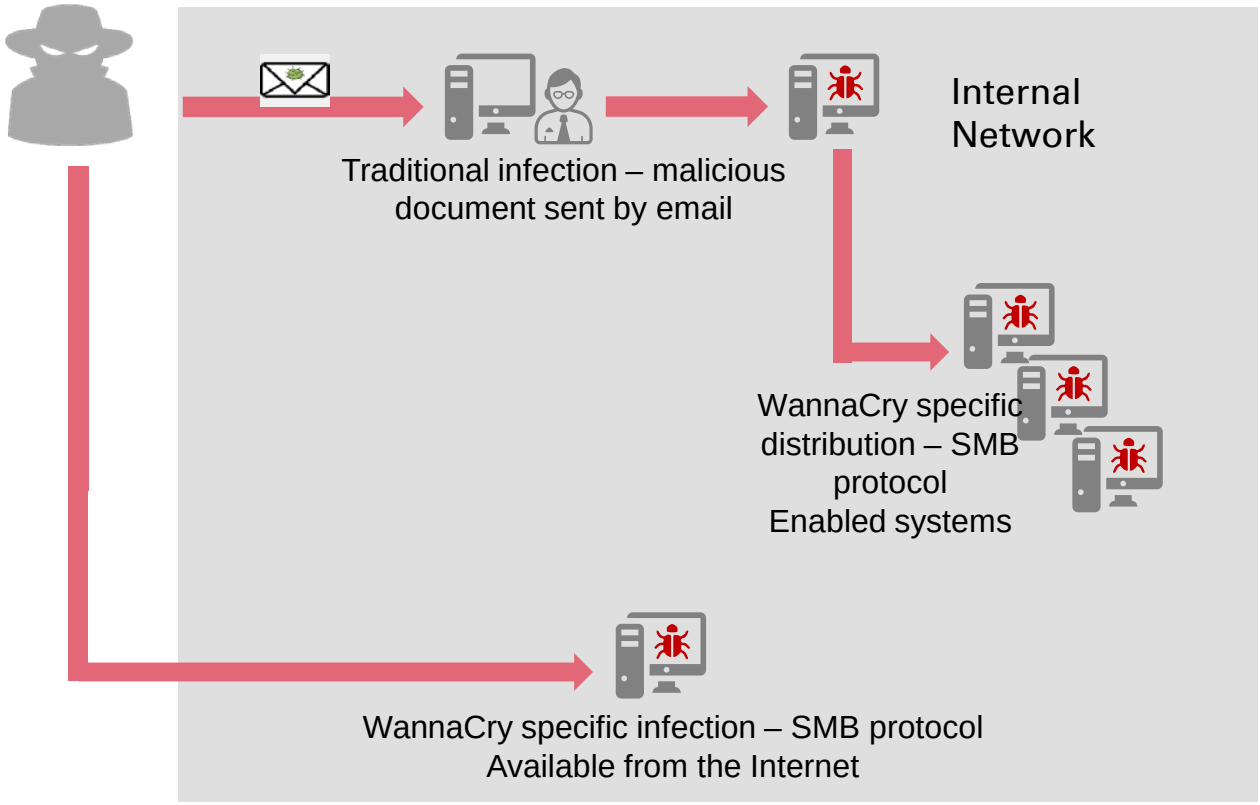
Modus Operandi

Das Verständnis wie Hacker heute vorgehen, womit und wie sie arbeiten .

Malware Infektion



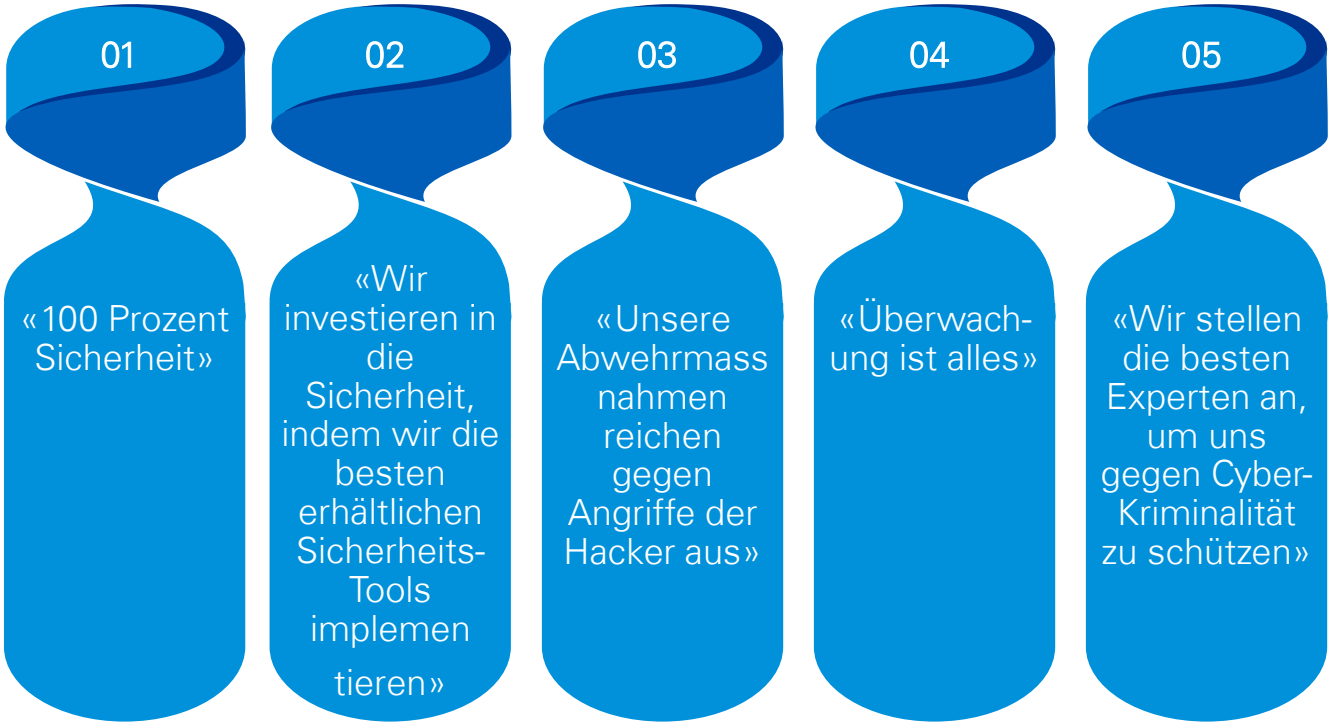
Erpressung - Ransomware



Schutzmassnahmen

Es braucht ein Netzwerk um ein Netzwerk zu bekämpfen…

Cyber-Sicherheit: Die fünf grössten Irrtümer



«Die 4 Goldenen Regeln» für Cyber Security

1. Wenden Sie Grundschutzmassnahmen an.
2. Sichern Sie Ihre «Crown Jewels».
3. Wer sind die Täter und was ist deren Motivation?
4. Nutzen Sie Cyber Security als Möglichkeit, Ihr eigenes Geschäft zu durchleuchten und Vertrauen zu schaffen

Grundschutzmassnahmen

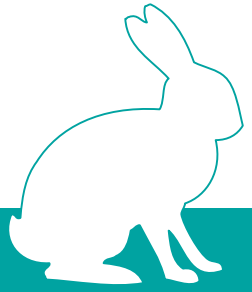
1) **Zuweisen von Rollen und Verantwortlichkeiten** für die Informations- und Systemsicherheit
2) **Kennen der eigenen Kronjuwelen** und Verstehen vom Cyber-Risiken-Gefährdungspotenzial
3) **Verstehen, welche Systeme im Netz vorhanden sind**, Löschung von verdächtigen oder Legacy-Systemen.
4) **Zugriffsbeschränkung** auf Daten und Systeme für die Mitarbeiter und Dritte
5) **Netzüberwachung und Segmentierung** und sicherer externer Zugriff via Firewalls, VPN, Zwei-Faktor-Authentifizierung
6) Regelmässiges **Patchen von Systemen** und **Überprüfung auf Malware**
7) **Durchführung von Sensibilisierungskampagnen** und Training für ALLE Benutzer zum Thema Sicherheit
8) **Durchführung von periodischen Sicherheitsprüfungen**
9) **Sicherstellung des eingebauten Sicherheit und Datenschutzes**
10) **Back-up** von Daten und Systemen-Konfiguration
11) **Aufbauen und Testen von Reaktionsplänen für Cyber-Vorfälle**

Wechselspiel zwischen Prävention, Erkennung und Reaktion

Erkennung

Response

Geschwindigkeit



Vorreiter

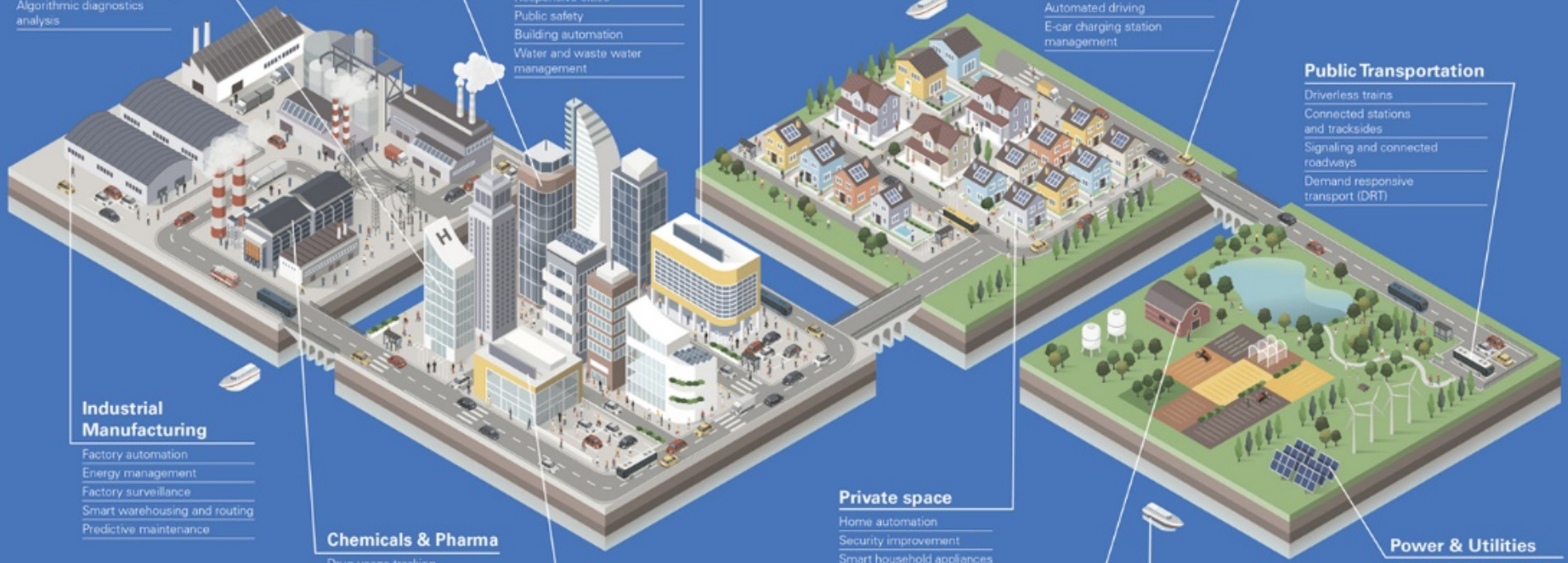
Eine Anzahl von Schweizer Unternehmen schafft es zumindest mit der Geschwindigkeit der sich entwickelnden Bedrohungs-Landschaft mitzuhalten. Die am weitesten fortgeschrittenen Unternehmen können die Risiken erfolgreich reduzieren und die getroffen Massnahmen nutzen, um neue Geschäftsfelder zu erschliessen und effizientere Betriebsmodellen einzuführen (z.B. Digitalisierung).

Spätzünder

Andere Unternehmen kämpfen mit der sich schnell entwickelnden Bedrohungslandschaft Schritt zu halten. Sie werden nicht in der Lage sein, ihre Geschäfte an die Risiken anzupassen und weiter zu entwickeln.

Das Internet der Dinge

There will be 20.8 billion devices connected to the Internet generating over 20 zettabytes of data by 2020.
(Source: Gartner)



Healthcare
- Remote patient observation
- Smart medical devices
- Smart prescription management
- Algorithmic diagnostics analysis

Banking & Insurance
- Mobile payment and wallets
- Smart ATMs
- Predictive insurance modeling
- Driving data recorder

Smart City
- Video surveillance
- Predictive policing
- Smart management of city infrastructure
- Responsive cities
- Public safety
- Building automation
- Water and waste water management

Individual Mobility
- GPS
- Car sharing
- Automated driving
- E-car charging station management

Public Transportation
- Driverless trains
- Connected stations and tracksides
- Signaling and connected roadways
- Demand responsive transport (DRT)

Industrial Manufacturing
- Factory automation
- Energy management
- Factory surveillance
- Smart warehousing and routing
- Predictive maintenance

Chemicals & Pharma
- Drug usage tracking
- Chronic disease management
- Smart pills

Consumer Goods & Retail
- Connected retail
- In-store localization
- Beacon technology
- Connected clothing

Private space
- Home automation
- Security improvement
- Smart household appliances

Agriculture
- Automated field testing
- Automated weeding

Transport & Leisure
- GPS and RFID
- Environment monitoring and management
- Responsive and adaptive supply chains
- Reservation, toll, and ticketing systems
- Guidance and control systems

Power & Utilities
- Supervisory control and data acquisition (SCADA)
- Advanced metering infrastructure (AMI)

Die 4. Industrielle Revolution erhöht den Einsatz von Cyber Security...

Cyber Security stärkt die Widerstandsfähigkeit unserer Gesellschaft, unserer Wirtschaft und unserer individuellen Gesundheit und Sicherheit.

Zusammenfassung

Cyber Angriffe sind «**Business as usual**»

Kennen und befolgen der **«4 Goldenen Regeln»**

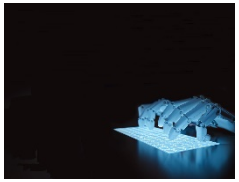
Kenne deinen Feind

Verständnis der Motivation, Strategie, Taktik und Mittel der Angreifer

Schutzmassnahmen

Kennen und befolgen der **«4 Goldenen Regeln»**

Kennen die fünf grössten Irrtümer



Ausblick

Widerstandsfähigkeit unserer Gesellschaft, unserer Wirtschaft und unserer individuellen Gesundheit und Sicherheit.

Fragen?

Ihr Referent

Roman Haltinner
Director
Cyber Security Services
T +41 58 249 42 56
rhaltinner@kpmg.com

KPMG AG
Badenerstrasse 172
Postfach
CH-8036 Zürich

kpmg.ch/socialmedia

kpmg.com/app