Cyber Risiken aus Schweizer Sicht

SVV Fachkommission Haftpflicht Info-Tagung, Bern, 12. Juni 2019

Fabian Harmati, Senior Product Manager Financial Lines, Swiss Re
Dr. Philipp Hurni, Cyber Model Lead, Swiss Re Cyber Centre of Competence

Swiss Re

Überblick

Was sind die grössten Cyber Be-drohungen?

Wer hat welche Interessen?

Phishing als Einfallstor?

Cyber Angriffe in der Schweiz:

Datendiebstahl
Erpressung
Spionage

Welche Police schützt wie?

Warum haben wir nur wenig Schaden-Daten?

Wie gehen Kriminelle vor?

Wie funktioniert ein Angriff?

Was sind die grössten Risiken?

Datendiebstahl und Identitätsdiebstahl (Data Breach)

Erpressung
- Ransomware
- Cryptolock
- Denial of Services

Sabotage/Spionage
- häufig “state sponsored”

Cyber Versicherung

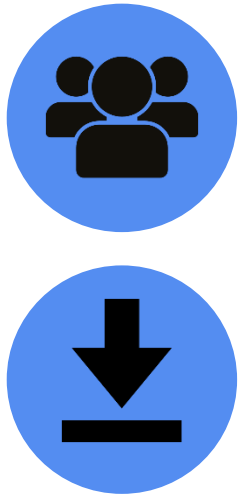
Wer hat welche Interessen? – Zahlen zum Thema Datenschutzverletzung

Menschliches Versagen

27%

System Fehler

25%



Cyber-Kriminelle

Hacktivisten "state sponsored" (Terroristen)

Script Kiddies Nerds White Hats

Unzufriedene Mitarbeiter

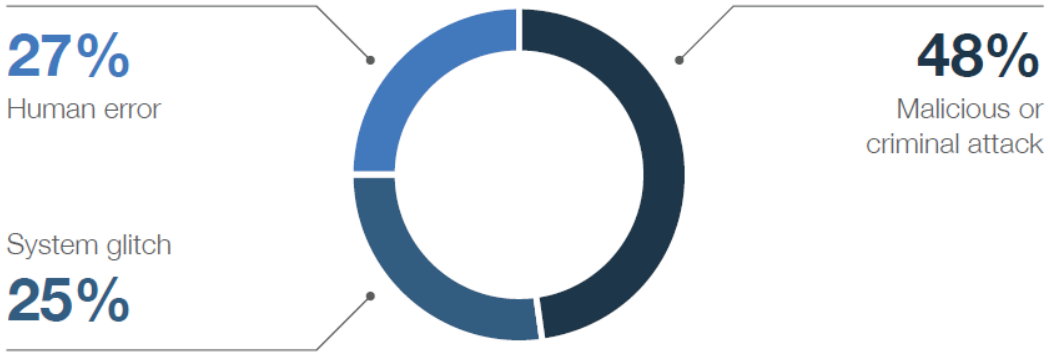
Finanzielle Interessen

Politisch/ Religiös

Spass/ Aufdeckung

Rache/ Finanz. Int.

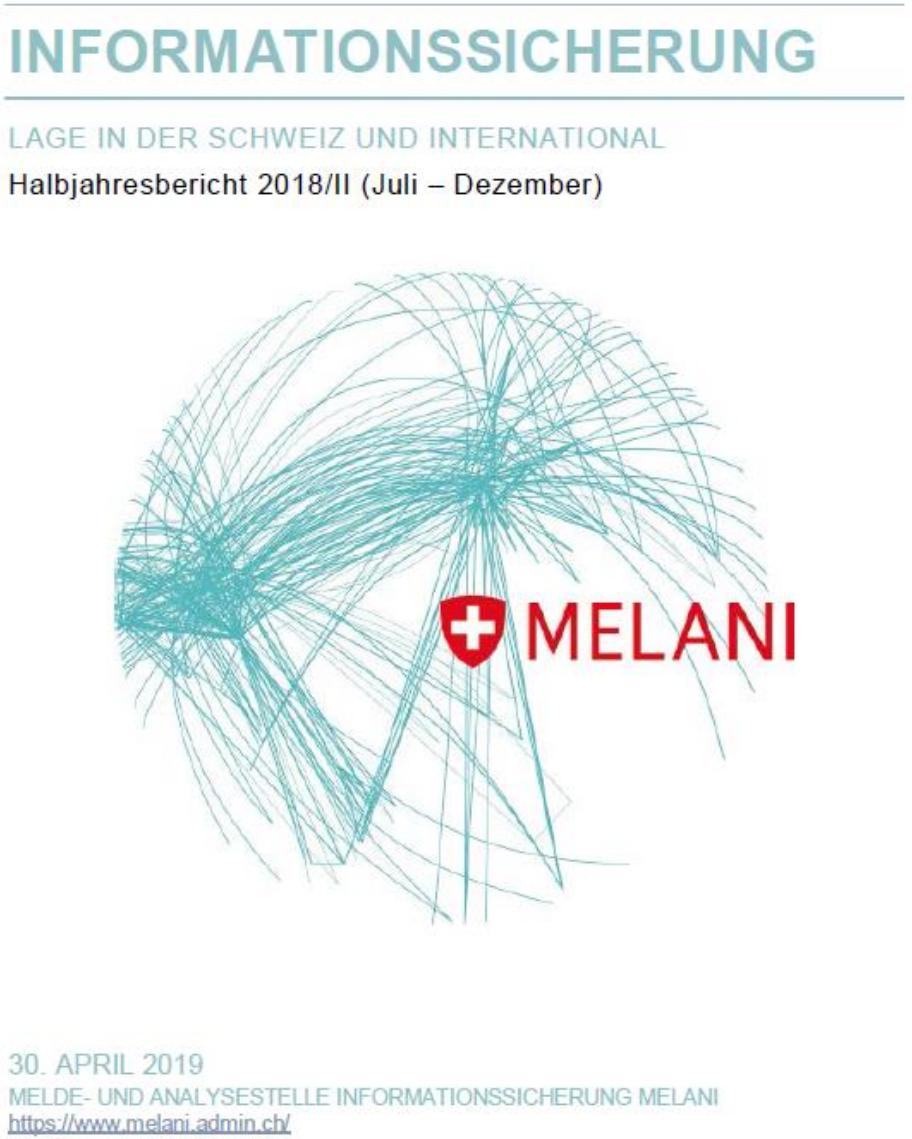
48%



Phishing als Einfallstor

- Im Jahr **2018** wurden **5756 verschiedene** eindeutige **Phishing-Seiten** über MELANI-Portal «antiphishing.ch» gemeldet.

Abbildung 3: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch in der zweiten Jahreshälfte 2018



Beispiele von Phishing Methoden – hätten Sie es bemerkt?

Gefälschter Absender

Di 30.05.2017 17:03

Christian Mumenthaler <execc@inbox.lv>

Confirm

To [redacted]

You forwarded this message on 30.05.2017 18:07.

There's something i need you to take care of,are you available?

Best Regards
Christian Mumenthaler

Gefälschte E-Mail-Adresse: anstatt ...@swissre.com

➔ @swisr**e**e.com

➔ @swi**i**sre.com

Was macht Schlagzeilen?

Hackers Used New Weapons to Disrupt Major Websites Across U.S.

PERLROTH OCT. 21, 2016

WannaCry ransomware cyber-attacks slow but fears remain

15 May 2017 | Technology Share

German Steel Mill Meltdown: Rising Stakes in the Internet of Things

POST STOLEN ASHLEY

Cyber-Angriffe in der Schweiz

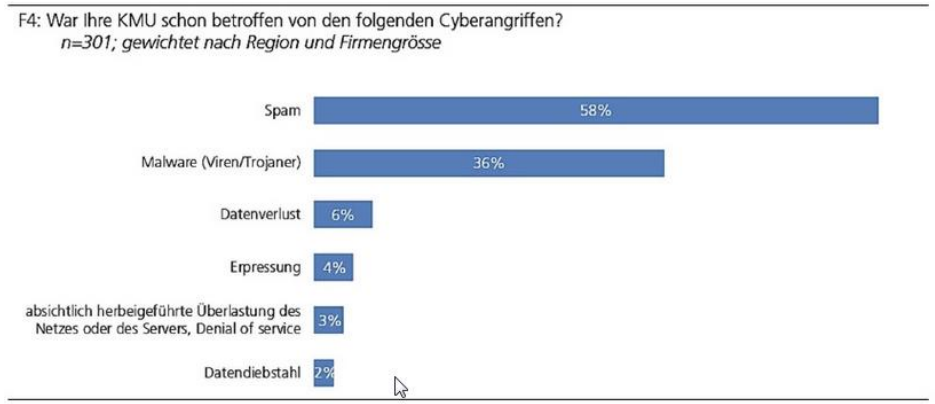
- **Dezember 2017**: SVV, SQS, ICTswitzerland und ISSS haben eine **Studie zur Cybersicherheit bei KMUs** vorgelegt.
- Mehr als **jedes dritte Schweizer KMU** wurde schon einmal Opfer von Cyberattacken.
- Hochgerechnet auf die Schweiz sind **23'000** KMUs **Opfer von Erpressungen** und über **200'000 von Schadsoftware** (Malware) betroffen gewesen.

Studie von ICTswitzerland

Schweizer KMUs unterschätzen das Risiko von Cyberangriffen

Di 12.12.2017 - 10:15 Uhr | Aktualisiert 12.12.2017 - 10:15
von Christoph Grau und Marcel Urech

SVV, SQS, ICTswitzerland und ISSS haben eine Studie zur Cybersicherheit bei KMUs vorgelegt. Mehr als jedes dritte Schweizer KMU wurde schon einmal Opfer von Cyberattacken. Dennoch schätzen Unternehmensentscheider die Gefahr nicht allzu hoch ein.



Beispiel Datendiebstahl

- **Februar 2018**: **800’000 Kundendatensätze** aus **Swisscom** Firmennetzwerk gestohlen.
- Einfallstor **gestohlene Zugriffsinformationen** eines Vertriebspartners.
- **Forensische Ermittlungen** hätten bisher ergeben, dass die Täter eine **französische IP-Adresse** nutzten.
- Weitere Ermittlungen verliefen im Sand.

Tages-Anzeiger

Swisscom-Leck: «Fahrlässig, wie die Daten gesichert waren»

Bei den gestohlenen 800'000 Kundendaten handle es sich um sensible Informationen, kritisiert der Zürcher Datenschützer die Swisscom.

https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/swisscom-verschaerft-sicherheitsmassnahmen/story/27504931

Beispiel Cyber-Erpressung

- **April 2019**: Cyberangriff auf die **Aebi Schmidt Gruppe** in Frauenfeld.
- Grosse Anzahl der **IT-Systeme** von **Schadsoftware** (Malware) «LockerGoga» betroffen.
- **Firmennetzwerk** fiel für **mehrere Tage** weitestgehend aus.
- Versuch mittels **Erpressung** ein **Lösegeld** zu fordern.

Tages-Anzeiger

Spuhler-Firma kämpft mit mysteriöser Hackerattacke

Der Schweizer Industriekonzern Aebi Schmidt bestätigt, dass er von einem Virus betroffen ist.

https://www.tagesanzeiger.ch/wirtschaft/spuhlerfirma-kaempft-mit-mysterioeser-hackerattacke/story/24988408

Beispiel Cyber-Spionage

- **Juli 2018**: Cyberangriff auf das **Labor Spiez**.
- Als Einfallstor wurden via **Phishing-Mails** Word-Dokumente **mit Schadsoftware** (Malware) versendet.
- Das **Forschungsinstitut** im Berner Oberland war an Analysen im **Vergiftungsfall des Ex-Doppelagenten Sergei Skripal** beteiligt.
- Hinter dem Angriff soll die **Hackergruppe «Sandworm»** stehen. Sie wird dem **russischen Militärgeheimdienst** GRU zugeordnet.

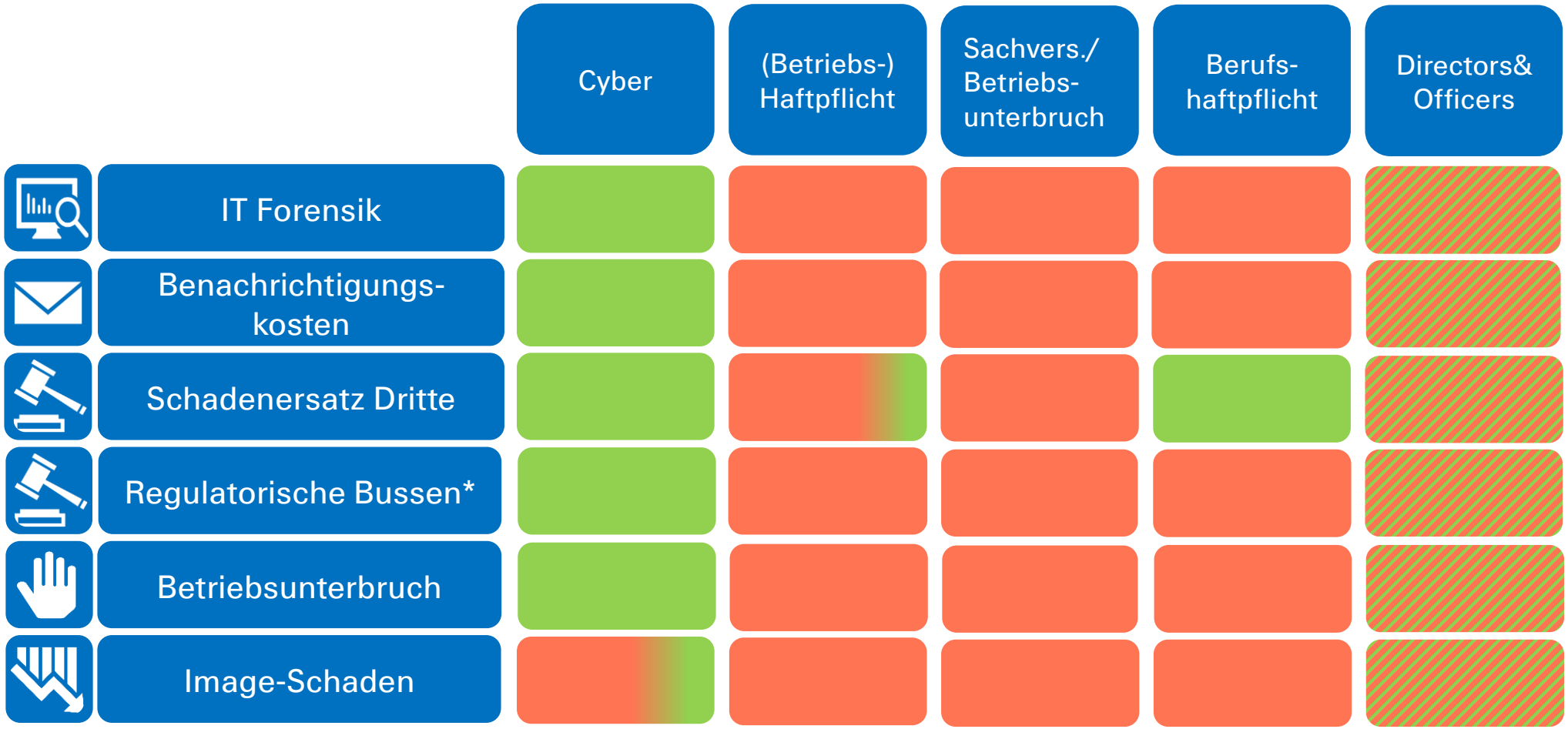
Tages-Anzeiger

Russische Hacker greifen Labor Spiez an

Die VBS-Fachstelle für biochemische Waffen ist erneut ins Visier von Russland geraten. Das Labor ermittelt sowohl in der Skripal-Affäre als auch beim Einsatz von Giftgas in Syrien.

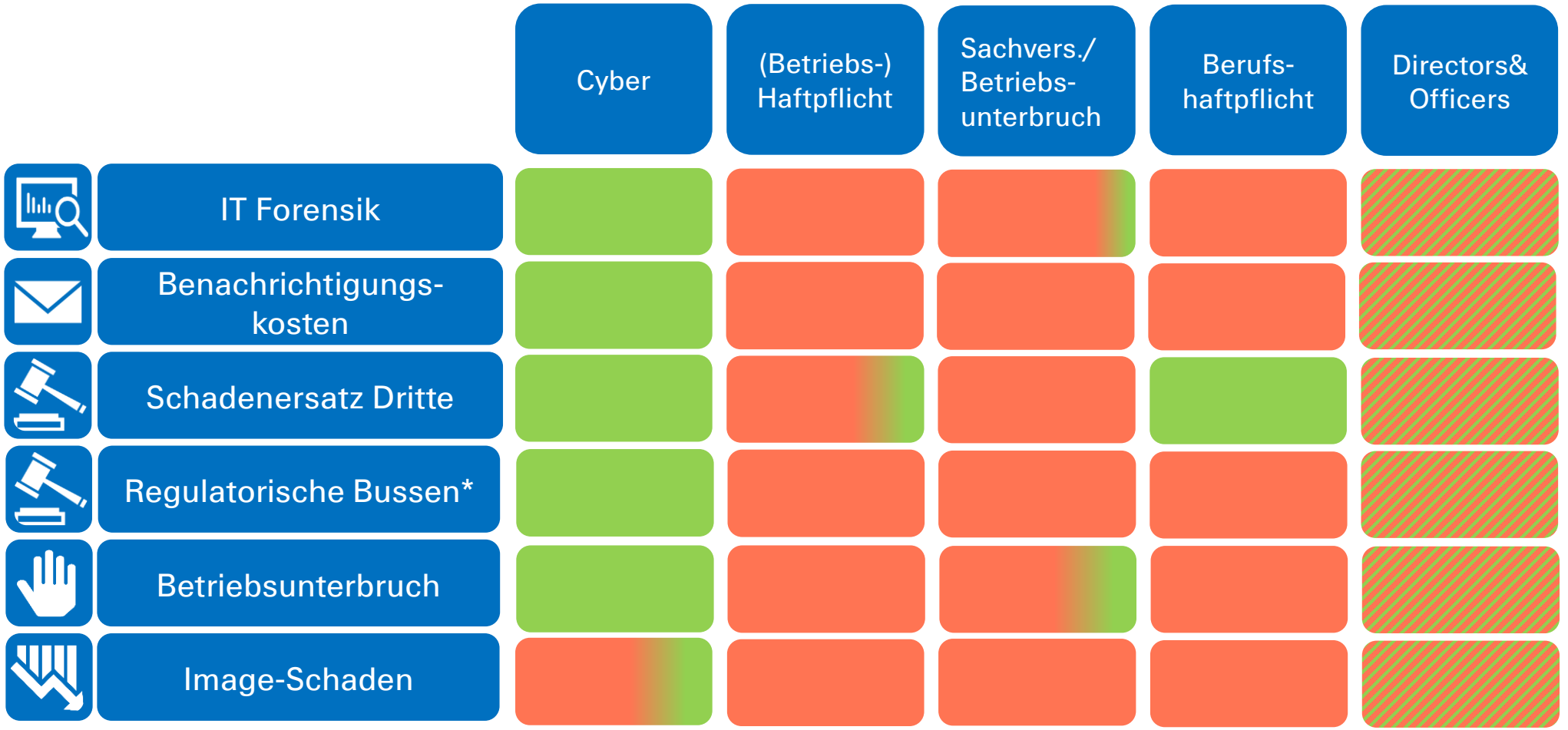
https://www.tagesanzeiger.ch/schweiz/standard/russische-hacker-greifen-labor-spiez-an/story/10982180

Beispiel 1: Deckungen bei einem Datendiebstahl (Data Breach)



* soweit versicherbar

Beispiel 2: Deckungen bei einer Erpressungsattacke (z.B. Ransomware)



* soweit versicherbar

Warum haben wir wenig Schaden-Daten?

- **Eine Million** Personen aus der **Schweiz** schon **von Cyber-Angriffen** betroffen.
- **Finanzielle** Schäden, **Aufwände** zur Schadens-bereinigung oder **emotionale** Belastungen.
- **Die Hälfte** der Betroffenen **meint, ausreichend** informiert zu sein.
- **Cyberversicherungen** sind **relativ junge** Produkte.
- Bei den **meisten** Cyber-Zwischenfälle im KMU-Segment **wurde noch keine Cyber-Police abgeschlossen** welche **Deckung bieten würde**.

Neue Zürcher Zeitung

Giorgio V. Müller
10.1.2019, 19:09 Uhr

Cyberattacken gehören zum Geschäftsalltag – 40 Prozent aller Schweizer Firmen mittlerweile betroffen

Laut einer 2017 vom Forschungsinstitut «gfs-zurich» durchgeführten Erhebung l**eisten sich nur 12% der kleinen und mittelgrossen Firmen eine Cyberversicherung**, obwohl viele bereits Opfer von Cyberattacken geworden sind. Die **Schwierigkeit** dabei ist, dass **es für die Tarifierung an Erfahrungswerten mangelt**.

https://www.nzz.ch/wirtschaft/cyberattacken-gehoeren-zum-geschaeftsalltag-ld.1450578

Schweizer KMU – was kann passieren?

- Beispiel Modebranche
- Umsatz 10 Mio – 40% online
- Kundenkartei mit 20’000 Kundenadressen
- 10’000 CHF Umsatz pro Tag
- Spitzentage ~ 100’000 CHF Umsatz pro Tag

Datendiebstahl der Kundenkartei
⇨ Aufwände für IT Spezialisten
⇨ Information der Kunden
⇨ Meldung an Aufsichtsbehörde
⇨ Geldbusse möglich bis 4% des Jahresumsatzes

Ransomware / Cryptolocker Office IT
⇨ Aufwände für IT Spezialisten
⇨ Mehraufwände/Betriebsunterbruch

Denial of Service Angriff auf Webshop
⇨ Aufwände für IT Spezialisten
⇨ Mehraufwände
⇨ Betriebsunterbruch, Umsatzeinbruch

Denial of Service Angriff

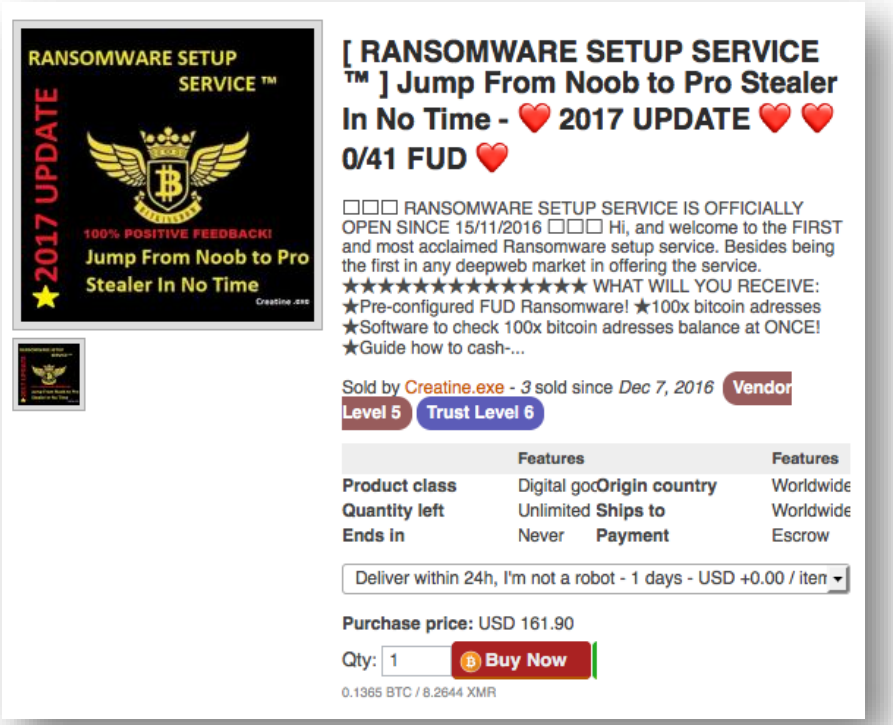
ein gängiges Angriffsmuster von Cyberkriminellen

Professionalisierung der Geschäftsmodelle im Bereich Cyberkriminalität

- Cyberkriminalität hat sich «professionalisiert»
- Cyberkriminelle können im «Cyber Untergrund» sehr schnell, einfach und günstig Werkzeuge und Dienstleistungen einkaufen, um Cyberangriffe zu lancieren
- Das “Darknet” wird benutzt als Marktplatz für solche Dienstleistungen
- Darknet: Internet-basierte Netzwerktechnologie, mit welcher Akteure **anonym** Informationen und Dienstleistungen austauschen können

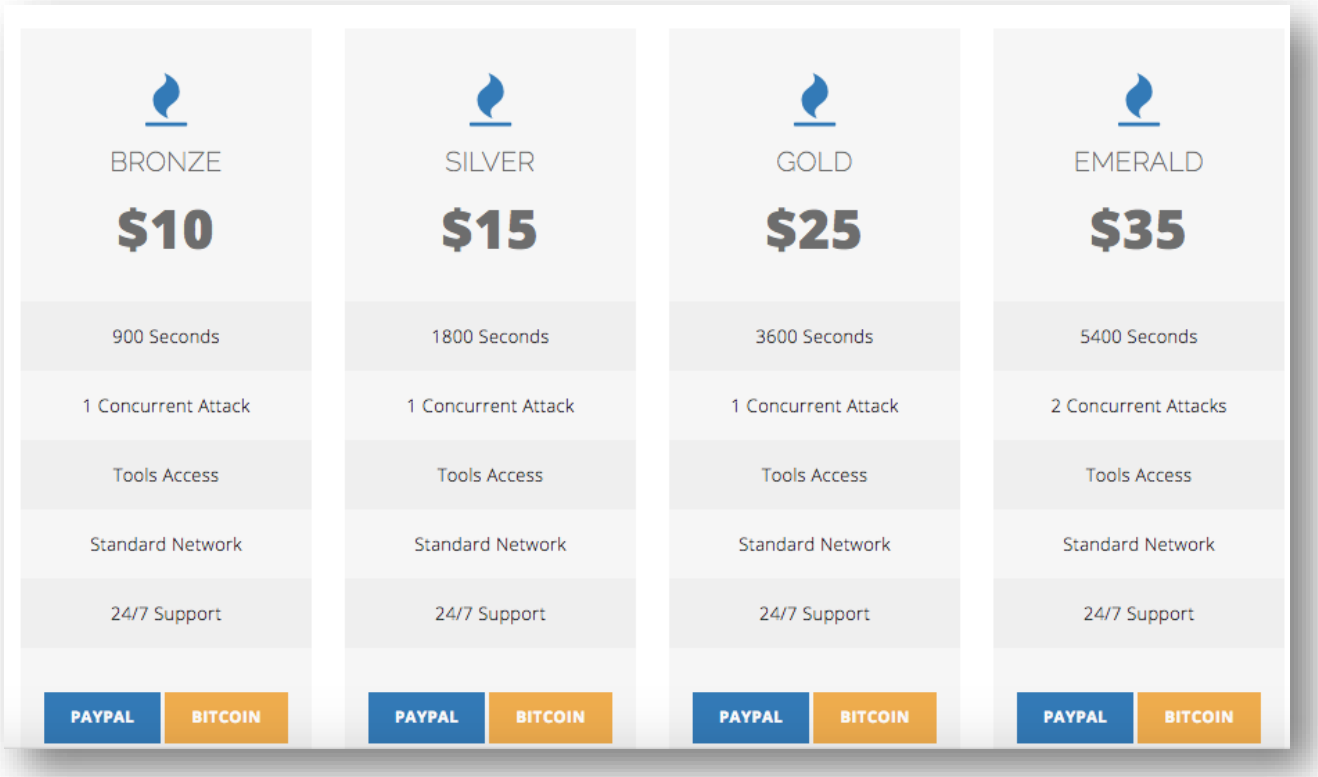
⇨ man muss kein absoluter IT-Professional sein, um in das “Geschäft” als Cyberkrimineller einzusteigen.

⇨ Dank Professionalisierung ist die “Eintrittsschwelle” tief

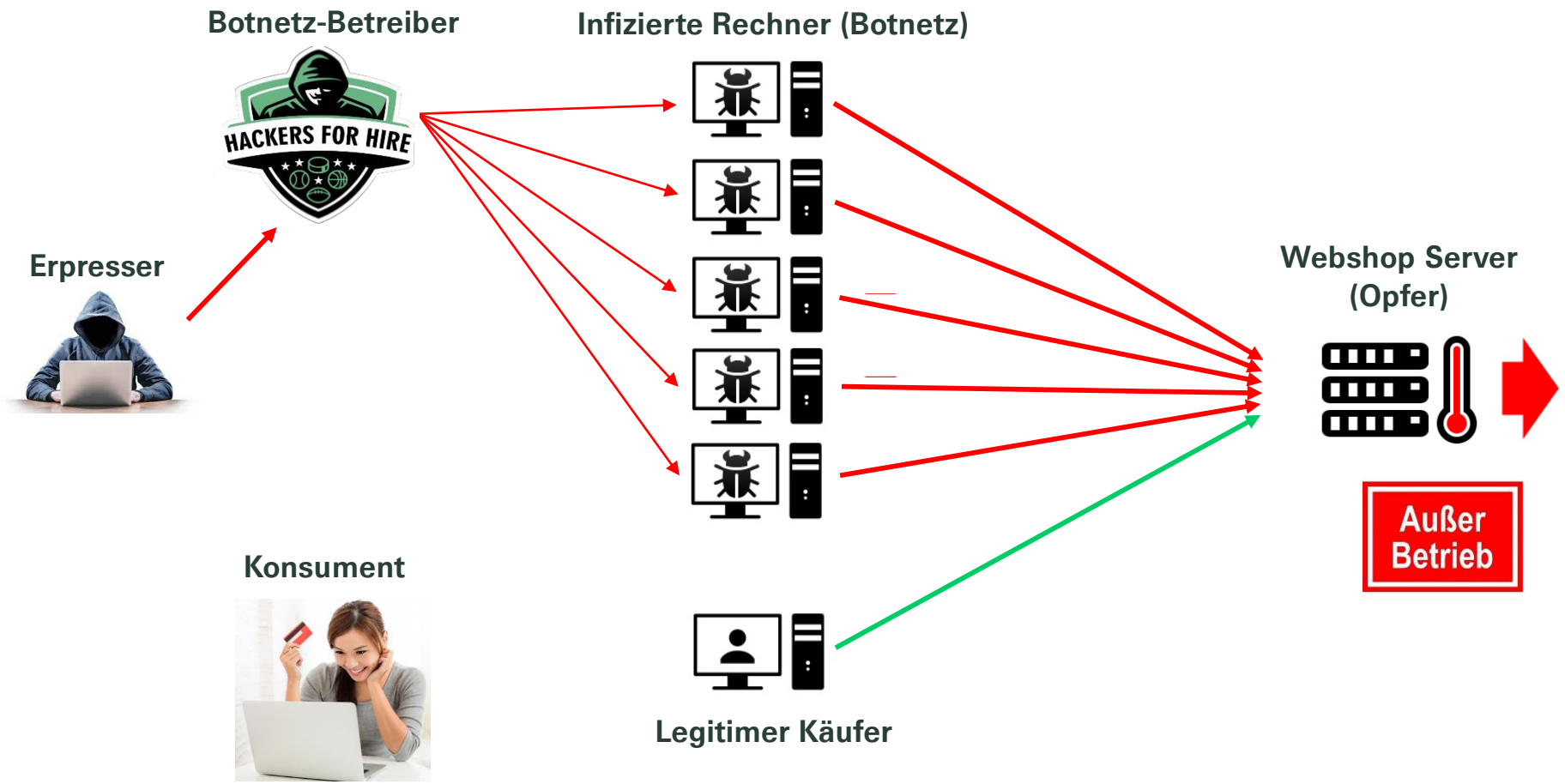


Denial-of-Service Angriff As-A-Service

- Denial-of-Service Angriffe können im Darknet mit wenigen Mausklicks “bestellt” werden
- Breite Produktepalette - Bezahlung via Bitcoin oder Paypal und 24/7 technischer Support



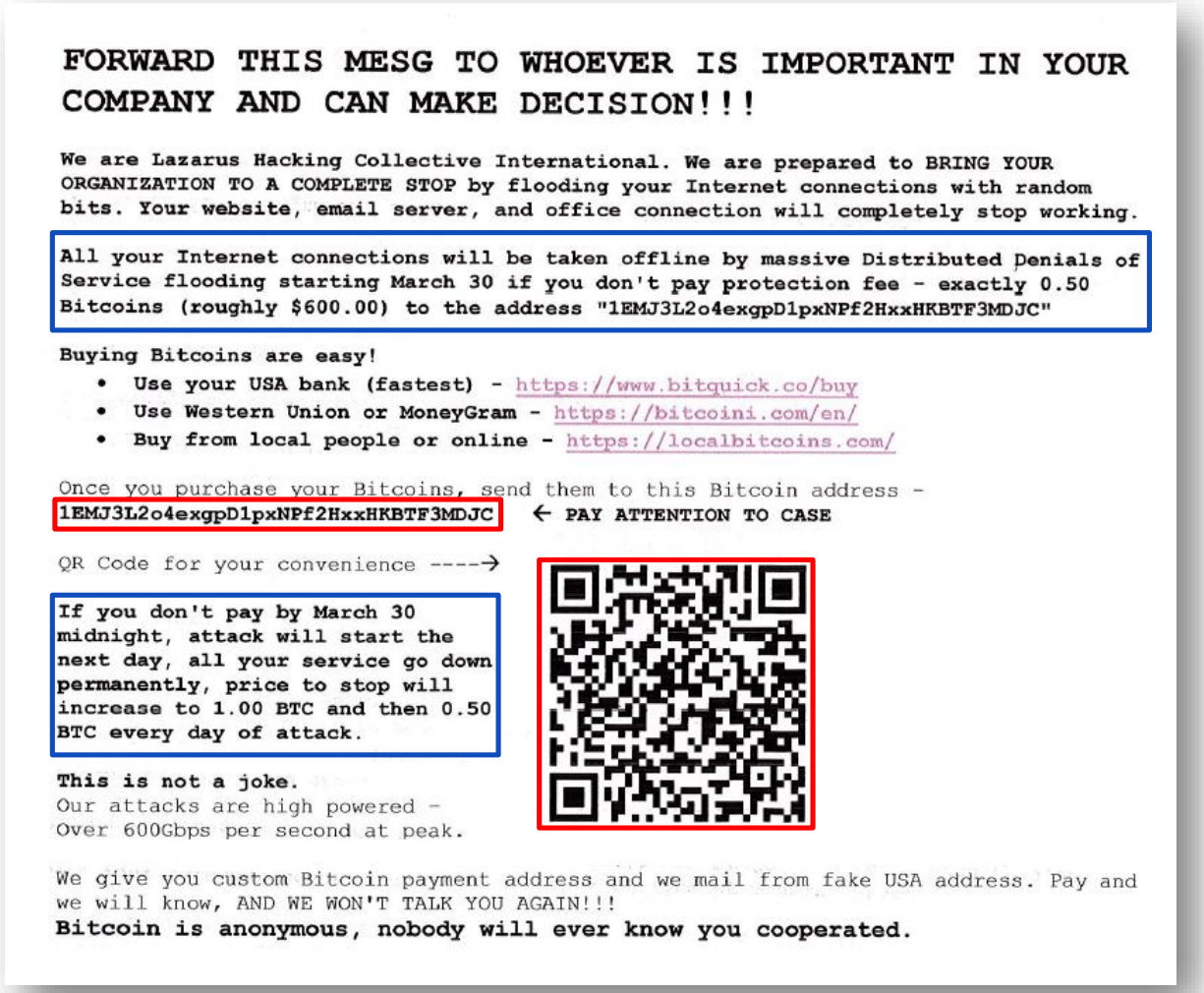
Denial of Service Angriff



Webshop erhält derart viele (illegitime) Anfragen, dass er nicht alle beantworten kann.

⇨ Er kann die Anfragen der legitimen Käufer nicht mehr erkennen und beantworten

Erpressung durch Androhung weiterer DDoS Attacken



FORWARD THIS MESG TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!!!

We are Lazarus Hacking Collective International. We are prepared to BRING YOUR ORGANIZATION TO A COMPLETE STOP by flooding your Internet connections with random bits. Your website, email server, and office connection will completely stop working.

All your Internet connections will be taken offline by massive Distributed Denials of Service flooding starting March 30 if you don't pay protection fee - exactly 0.50 Bitcoins (roughly $600.00) to the address "1EMJ3L2o4exgpD1pxNPf2HxxHKBTF3MDJC"

Buying Bitcoins are easy!

- **Use your USA bank (fastest) -** https://www.bitquick.co/buy
- **Use Western Union or MoneyGram -** https://bitcoini.com/en/
- **Buy from local people or online -** https://localbitcoins.com/

Once you purchase your Bitcoins, send them to this Bitcoin address -
1EMJ3L2o4exgpD1pxNPf2HxxHKBTF3MDJC ← **PAY ATTENTION TO CASE**

QR Code for your convenience ----→

If you don't pay by March 30 midnight, attack will start the next day, all your service go down permanently, price to stop will increase to 1.00 BTC and then 0.50 BTC every day of attack.

This is not a joke.
Our attacks are high powered -
Over 600Gbps per second at peak.

We give you custom Bitcoin payment address and we mail from fake USA address. Pay and we will know, AND WE WON'T TALK YOU AGAIN!!!
Bitcoin is anonymous, nobody will ever know you cooperated.

Androhung eines weiteren DoS Angriffs und Forderung einer Erpressungssumme

Bitcoin-Adresse zur Überweisung der geforderten Erpressungssumme

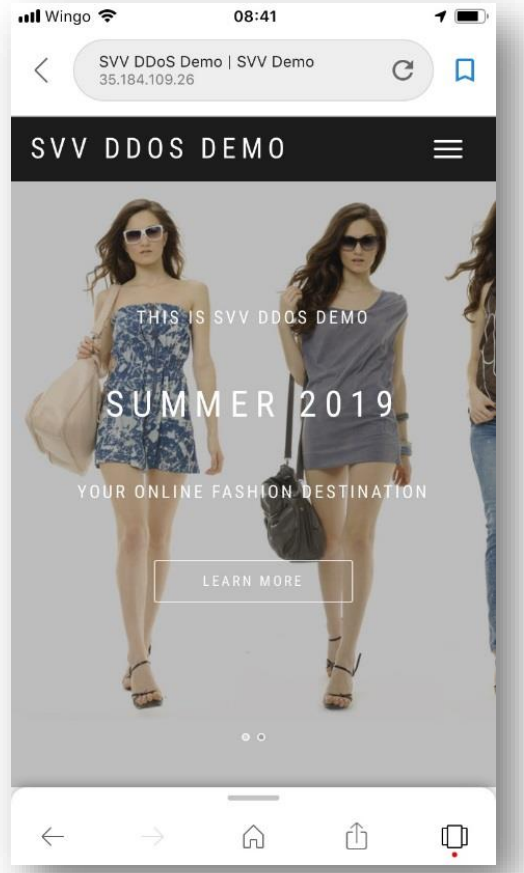
Lösegeldforderung steigt, je länger das Opfer zuwartet

Demonstration - Denial of Service Angriff

- “Opfer”: Dummy-Webseite mit Fashion Webshop
- Seite ist erreichbar via Web (www.hurni.org)
- Angreifer: gemietete virtuelle Maschinen (kein Botnetz!)
- Ziel des “Angriffs”: Solange der Angriff andauert, soll niemand mehr die Webseite erreichen können

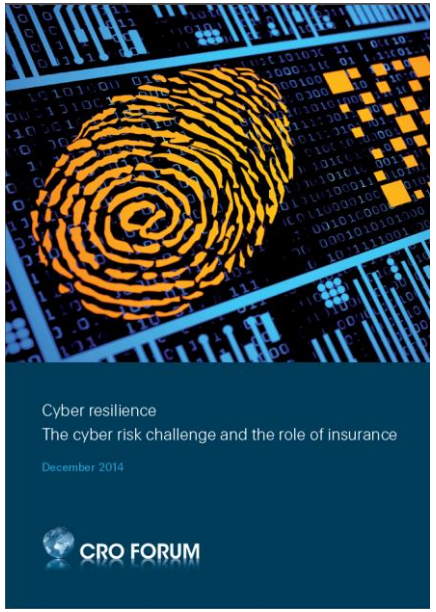
Wichtig !
Sämtliche verwendeten IT Ressourcen gehören mir selbst

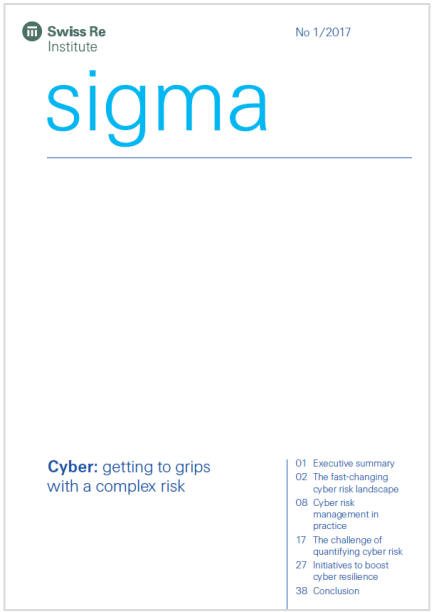
Niemand sonst ist von der Demonstration betroffen/“wird gehackt”

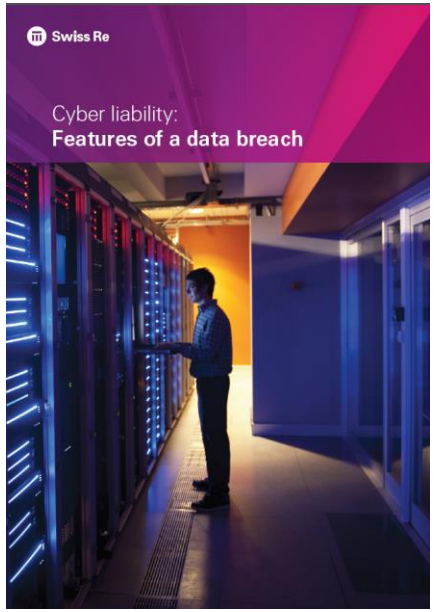


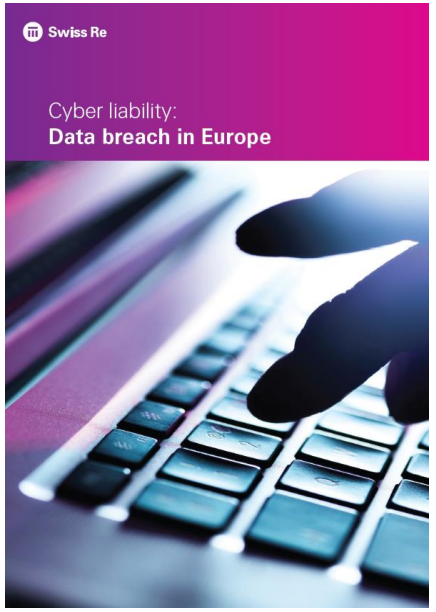
www.hurni.org

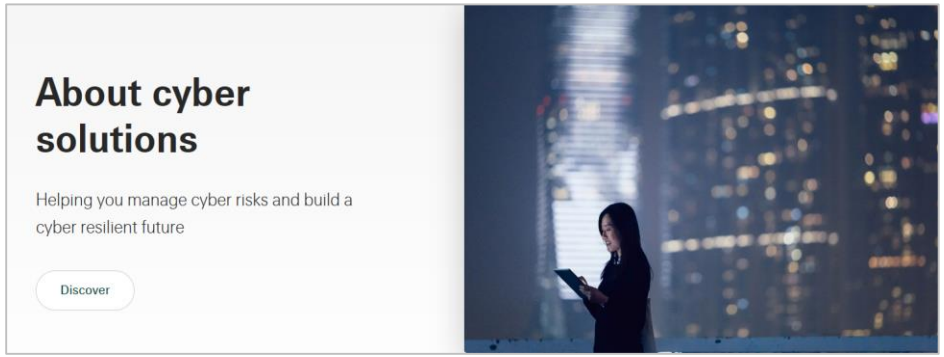
Haben wir Ihr Interesse geweckt?
Weitere Informationen finden Sie unter http://www.swissre.com/library

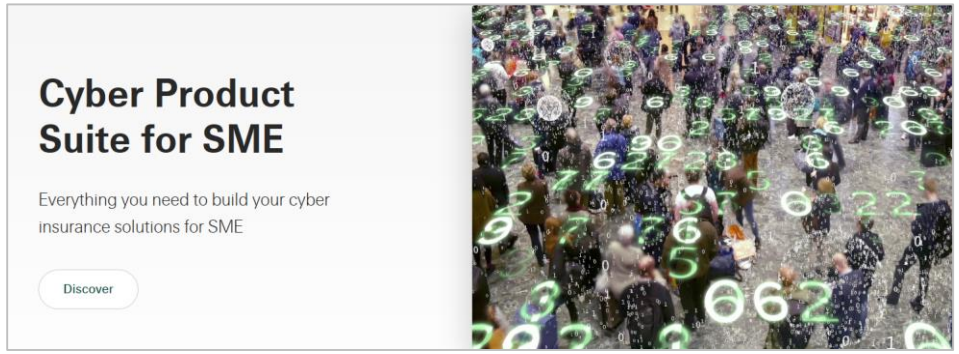












Haben Sie noch Fragen?

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.