

Cyber Risiken aus Schweizer Sicht

SWV 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

Überblick



Was sind die grössten Cyber Bedrohungen?

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



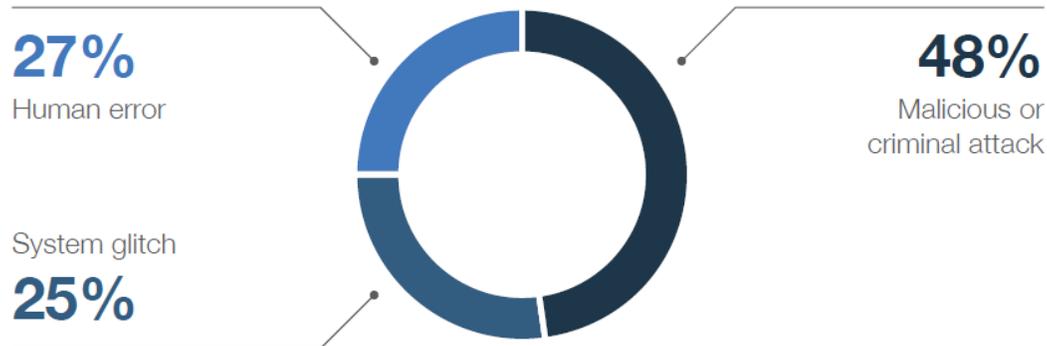
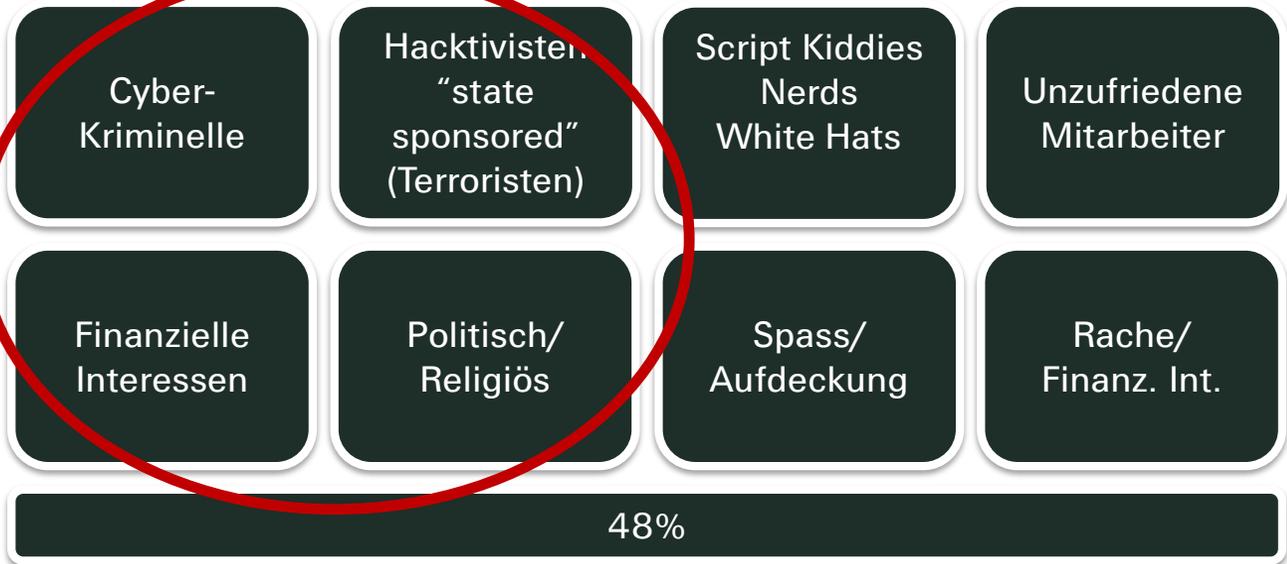
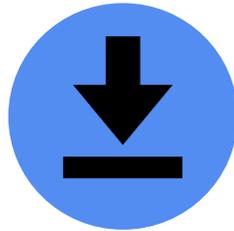
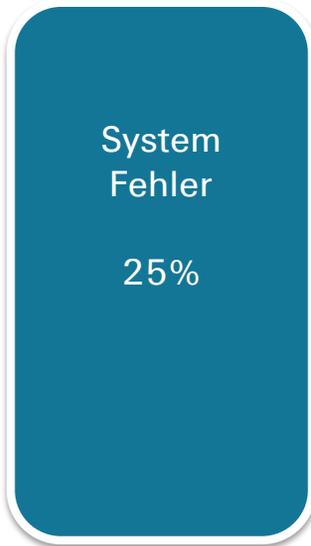
Sabotage/Spionage

- häufig "state sponsored"

Cyber Versicherung



Wer hat welche Interessen? – Zahlen zum Thema Datenschutzverletzung



Phishing als Einfallstor

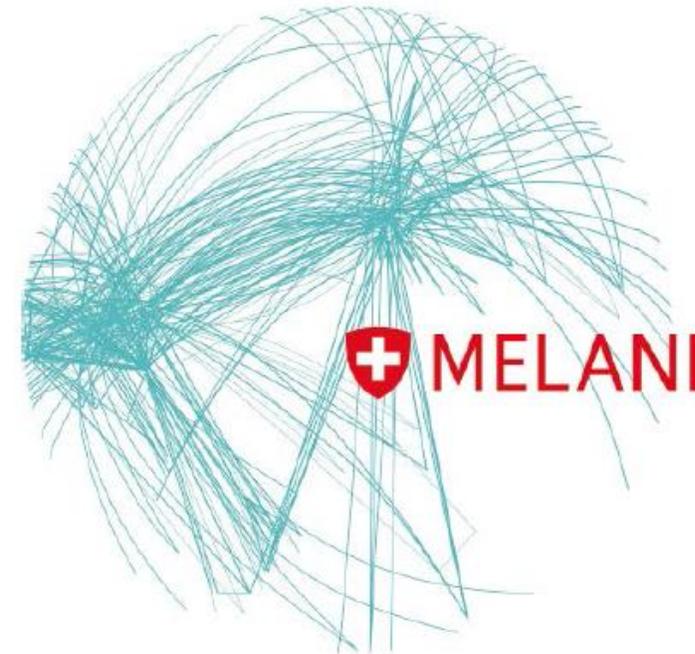
- Im Jahr **2018** wurden **5756** verschiedene eindeutige **Phishing-Seiten** über MELANI-Portal «antiphishing.ch» gemeldet.



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

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL
Halbjahresbericht 2018/II (Juli – Dezember)



30. APRIL 2019
MELDE- UND ANALYSESTELLE INFORMATIONSSICHERUNG MELANI
<https://www.melani.admin.ch/>

Beispiele von Phishing Methoden – hätten Sie es bemerkt?

Gefälschter Absender



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



Was macht Schlagzeilen?



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



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.

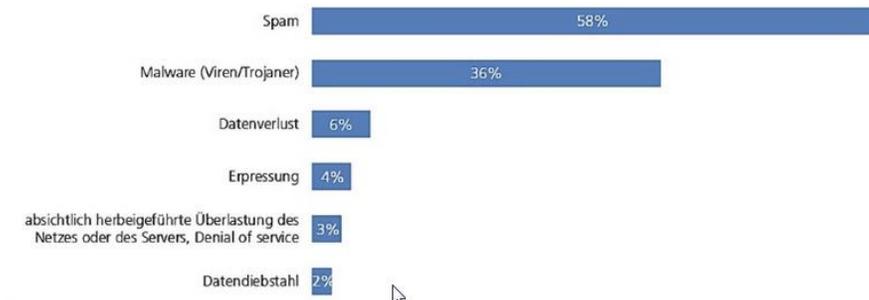
Studie von ICTswitzerland

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.

F4: War Ihre KMU schon betroffen von den folgenden Cyberangriffen?
n=301; gewichtet nach Region und Firmengrösse



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.

TagesAnzeiger

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.

TagesAnzeiger

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.

TagesAnzeiger

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)

		Cyber	(Betriebs-)Haftpflicht	Sachvers./Betriebsunterbruch	Berufshaftpflicht	Directors&Officers
	IT Forensik	Green	Orange	Orange	Orange	Diagonal Stripes
	Benachrichtigungskosten	Green	Orange	Orange	Orange	Diagonal Stripes
	Schadenersatz Dritte	Green	Orange	Orange	Green	Diagonal Stripes
	Regulatorische Bussen*	Green	Orange	Orange	Orange	Diagonal Stripes
	Betriebsunterbruch	Green	Orange	Orange	Orange	Diagonal Stripes
	Image-Schaden	Orange	Orange	Orange	Orange	Diagonal Stripes

* soweit versicherbar

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

		Cyber	(Betriebs-)Haftpflicht	Sachvers./Betriebsunterbruch	Berufshaftpflicht	Directors&Officers
	IT Forensik	Green	Orange	Orange	Orange	Diagonal lines
	Benachrichtigungskosten	Green	Orange	Orange	Orange	Diagonal lines
	Schadenersatz Dritte	Green	Orange	Orange	Green	Diagonal lines
	Regulatorische Bussen*	Green	Orange	Orange	Orange	Diagonal lines
	Betriebsunterbruch	Green	Orange	Orange	Orange	Diagonal lines
	Image-Schaden	Orange	Orange	Orange	Orange	Diagonal lines

* soweit versicherbar

Warum haben wir wenig Schaden-Daten?



- Eine Million Personen aus der Schweiz schon von Cyber-Angriffen betroffen.
- **Finanzielle** Schäden, **Aufwände** zur Schadensbereinigung 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-zürich» durchgeführten Erhebung leisten 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-gehoren-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



enSoie
ROTAUF



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



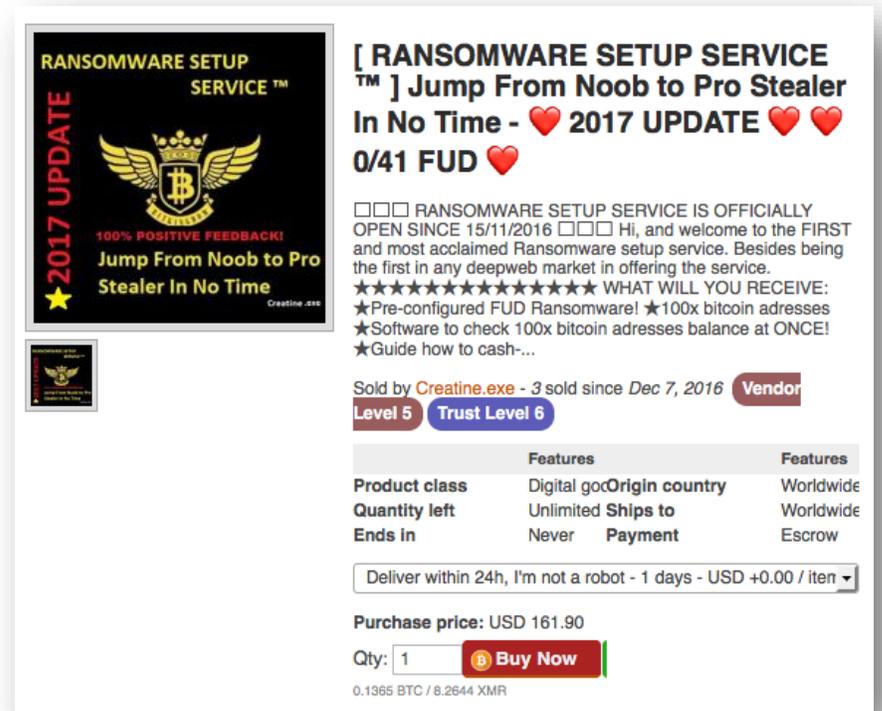
Denial of Service Angriff auf Webshop
⇒ Aufwände für IT Spezialisten
⇒ Mehraufwände
⇒ Betriebsunterbruch, Umsatzeinbruch

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



The screenshot shows a marketplace listing for 'RANSOMWARE SETUP SERVICE'. The main image features a Bitcoin logo with wings and the text 'RANSOMWARE SETUP SERVICE™', '100% POSITIVE FEEDBACK!', and 'Jump From Noob to Pro Stealer In No Time'. The listing text includes: '[RANSOMWARE SETUP SERVICE™] Jump From Noob to Pro Stealer In No Time - ❤️ 2017 UPDATE ❤️ ❤️ 0/41 FUD ❤️'. It also states 'RANSOMWARE SETUP SERVICE IS OFFICIALLY OPEN SINCE 15/11/2016' and lists features like 'Pre-configured FUD Ransomware!', '100x bitcoin addresses', and 'Software to check 100x bitcoin addresses balance at ONCE!'. The vendor is 'Creatine.exe' with a 'Level 5' badge and 'Trust Level 6'. A table of features is provided, and the purchase price is 'USD 161.90'.

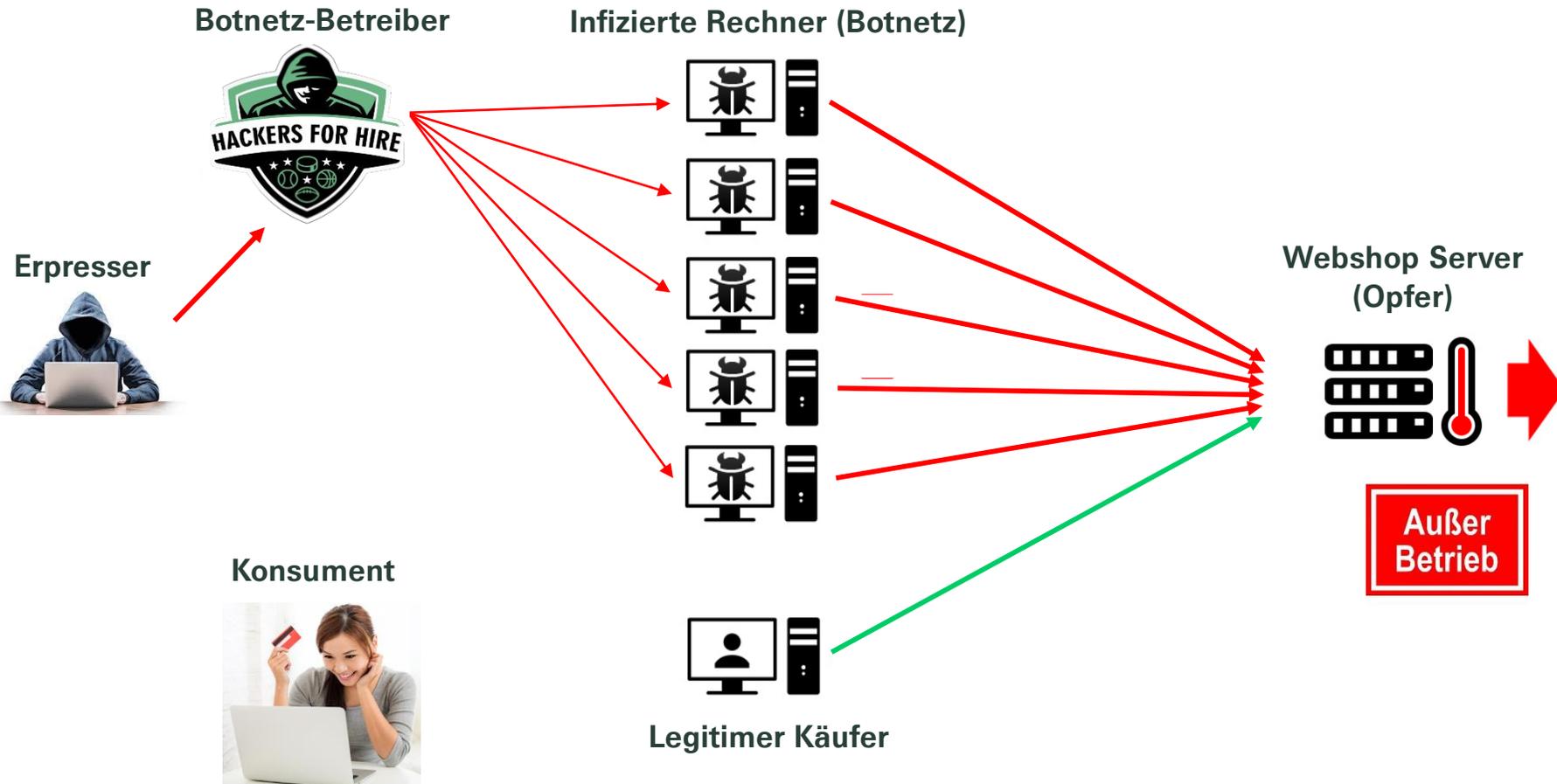
	Features	Features
Product class	Digital go	Origin country
Quantity left	Unlimited	Ships to
Ends in	Never	Payment
		Escrow

Denial-of-Service Angriff As-A-Service

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

 BRONZE	 SILVER	 GOLD	 EMERALD
\$10	\$15	\$25	\$35
900 Seconds	1800 Seconds	3600 Seconds	5400 Seconds
1 Concurrent Attack	1 Concurrent Attack	1 Concurrent Attack	2 Concurrent Attacks
Tools Access	Tools Access	Tools Access	Tools Access
Standard Network	Standard Network	Standard Network	Standard Network
24/7 Support	24/7 Support	24/7 Support	24/7 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 MESSG 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

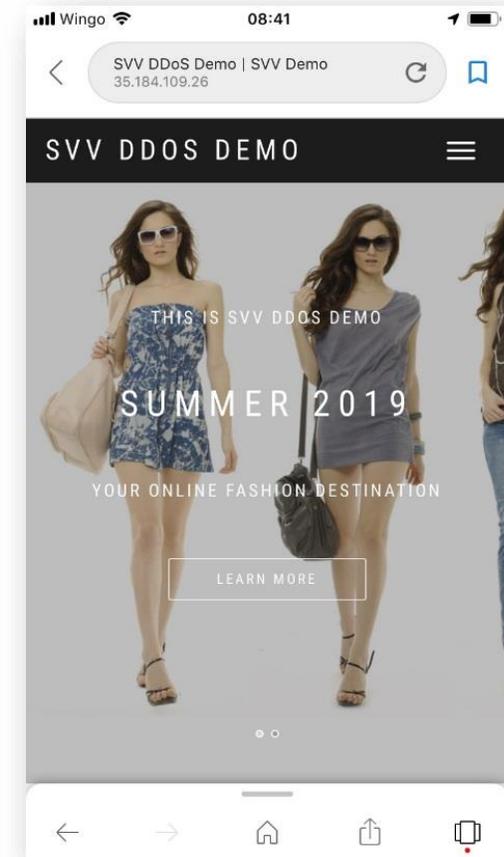
Demonstration - Denial of Service Angriff

- “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

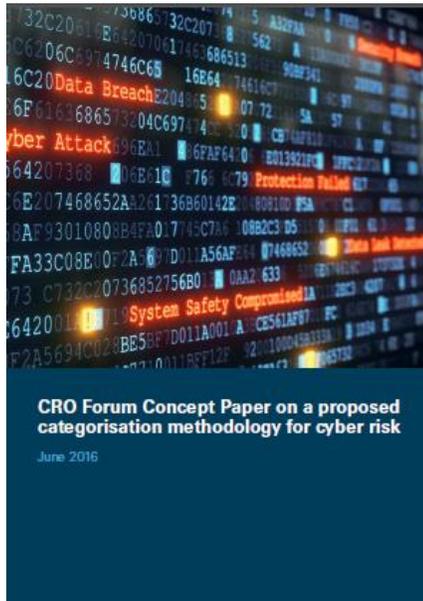
Niemand sonst ist von der Demonstration betroffen/“wird gehackt”



www.hurni.org

Haben wir Ihr Interesse geweckt?

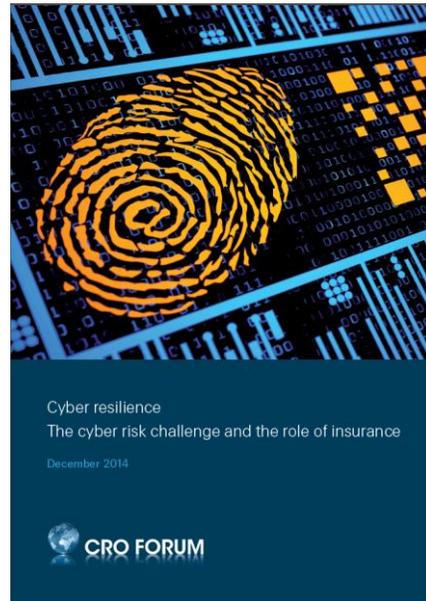
Weitere Informationen finden Sie unter <http://www.swissre.com/library>



CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk

June 2016

The cover features a dark background with glowing orange and yellow text and symbols, including "Data Breach", "Cyber Attack", and "System Safety Compromised".

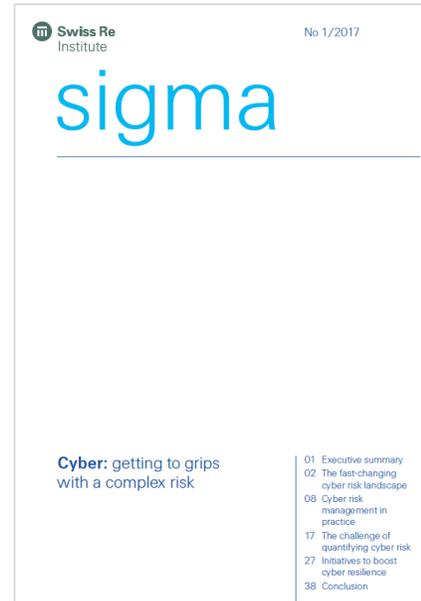


Cyber resilience
The cyber risk challenge and the role of insurance

December 2014

CRO FORUM

The cover features a glowing orange fingerprint graphic on a dark background with binary code.



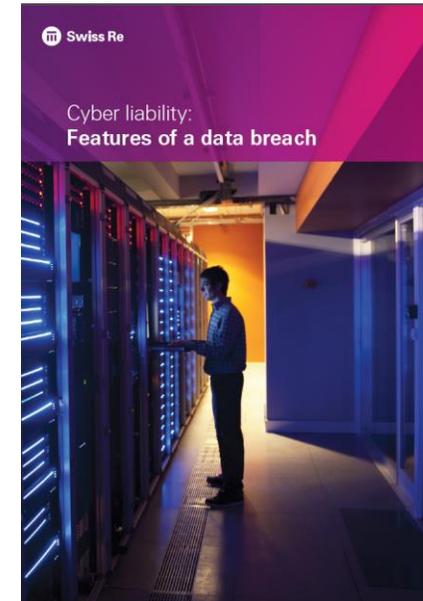
Swiss Re Institute No 1/2017

sigma

Cyber: getting to grips with a complex risk

- 01 Executive summary
- 02 The fast-changing cyber risk landscape
- 08 Cyber risk management in practice
- 17 The challenge of quantifying cyber risk
- 27 Initiatives to boost cyber resilience
- 38 Conclusion

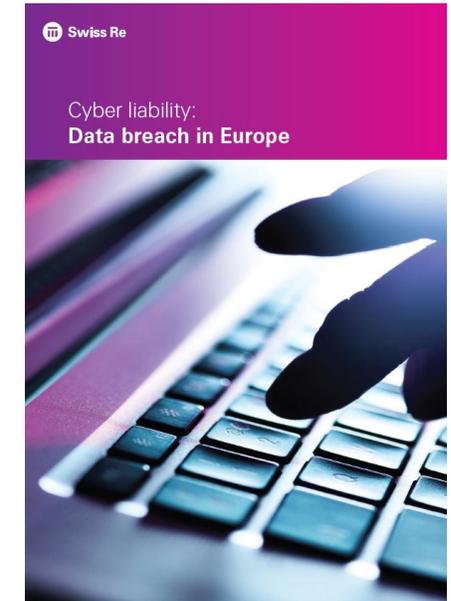
The cover is white with the word "sigma" in blue and a list of contents on the right side.



Swiss Re

Cyber liability: Features of a data breach

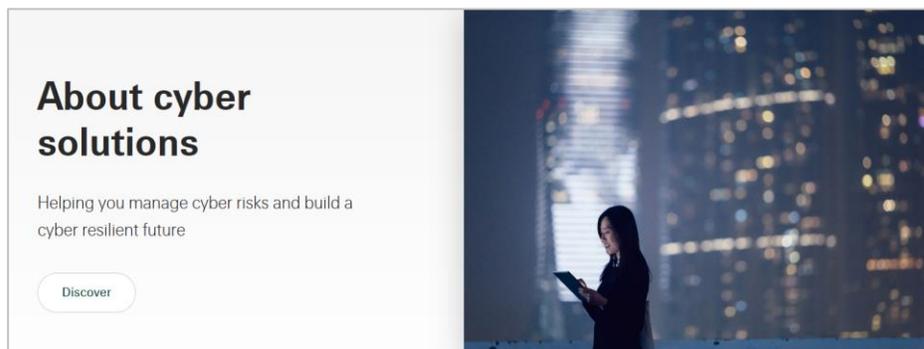
The cover features a photograph of a person standing in a server room with blue lighting.



Swiss Re

Cyber liability: Data breach in Europe

The cover features a close-up photograph of a hand typing on a laptop keyboard.

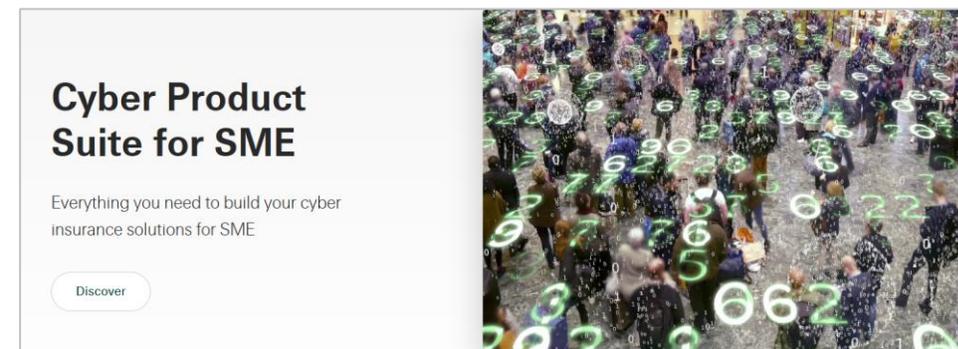


About cyber solutions

Helping you manage cyber risks and build a cyber resilient future

Discover

The cover features a photograph of a woman looking at a smartphone in front of a city skyline at night.



Cyber Product Suite for SME

Everything you need to build your cyber insurance solutions for SME

Discover

The cover features a photograph of a crowd of people with glowing green numbers floating around them.

Haben Sie noch Fragen?



Legal notice

©2019 Swiss Re. All rights reserved. You are not permitted to create any modifications or derivative works of this presentation or to use it for commercial or other public purposes without the prior written permission of Swiss Re.

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.