



Cyber Risk Resilience – Wirkungsvoller Ansatz gegen Cyber-Angriffe

Swiss Networking Day 2016

«Cyber Security ist vielschichtig.
Ein zuverlässiger Schutz Ihrer Werte –
Informationen, Mitarbeiter, Prozesse und
Infrastruktur – lässt sich nur über einen
strukturierten, methodischen Sicherheits-
prozess erreichen.»



Franco Cerminara

Head of Consulting

Member of the Management

InfoGuard AG

+41 41 749 19 62

+41 79 308 83 16

franco.cerminara@infoguard.ch

Tour de Sol 1987 von Biel - Arosa



A Member of The Crypto Group - Kompetenz seit 1952



- › Schweizer Cyber Security Spezialist
- › 60 Sicherheitsexperten
- › Kompetenz seit 1988
- › Über 300 zufriedene Kunden
- › ISO/IEC 27001:2013 zertifiziert
- › «The Crypto Group»: 300 Sicherheitsexperten und Kunden in 130 Ländern weltweit, gegründet 1952



Definition

Resilience: The ability of an ecosystem to return to its original state after being disturbed
(Collins Dictionary)

Resilience: The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents
(USA Department of Homeland Security)

Cyber resilience: The ability of systems and organisations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery
(World Economic Forum)

Cyber resilience: The organisation's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace
(Information Security Forum)

Cyber resilience:

1. Aufbau einer höheren Widerstandsfähigkeit gegenüber Cyberkriminalität.
2. Widerstandskraft eines Unternehmens gegen Angriffe auf die Informationssicherheit

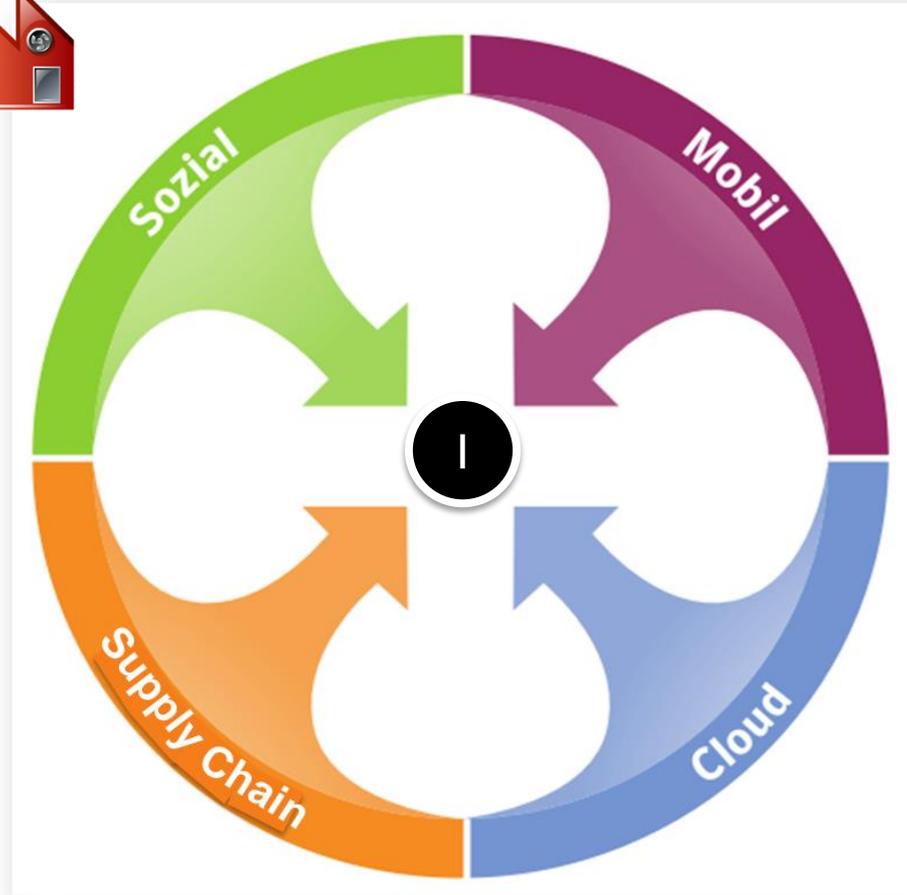
«Cyber Security» Früher



I = Informationen

Castle star in Portanj, Netherlands – Photo by Jan Koster

«Cyber Security» Heute

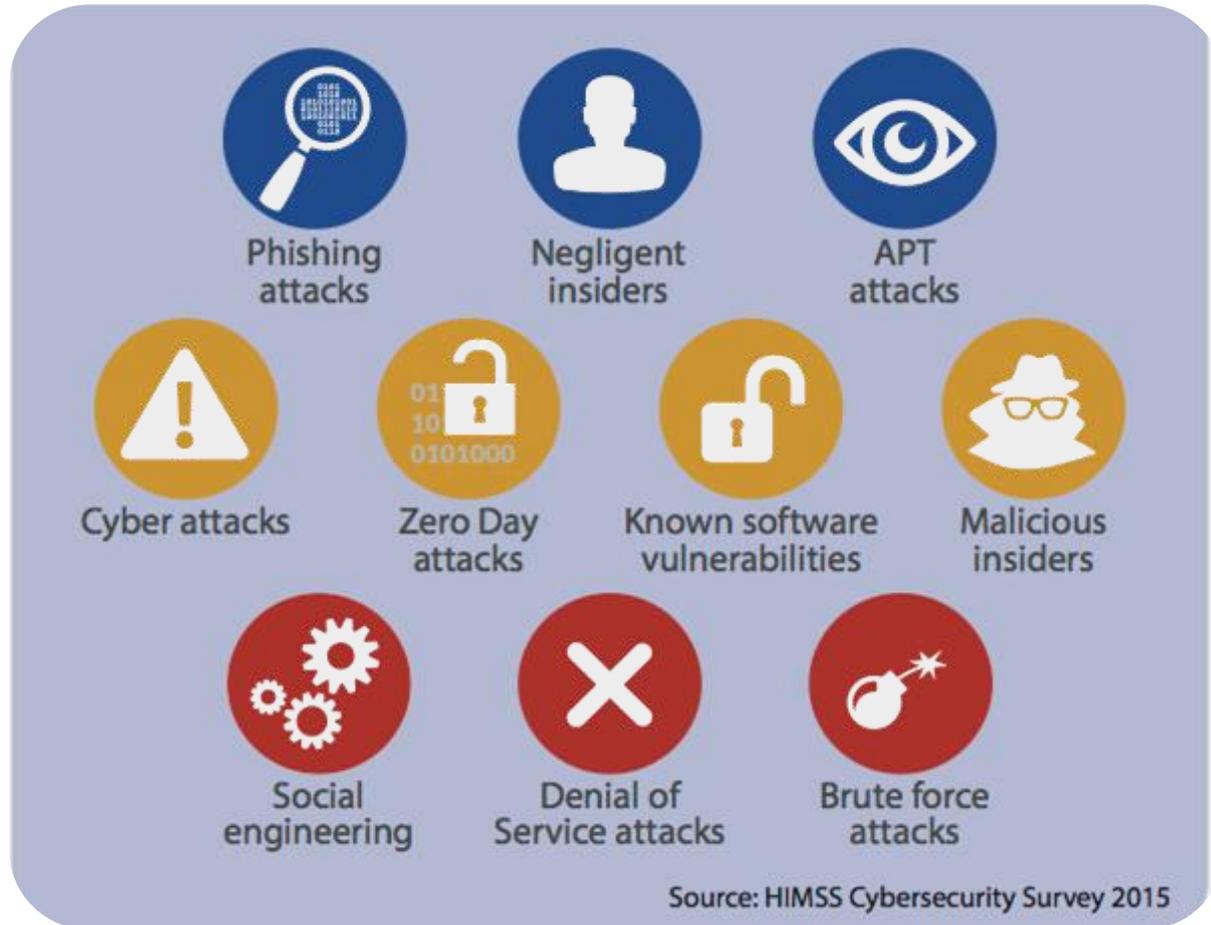


I = Informationen



Unternehmen sind heute verwundbarer durch Cyber Angriffe

«Top 10 Cyber Threats»

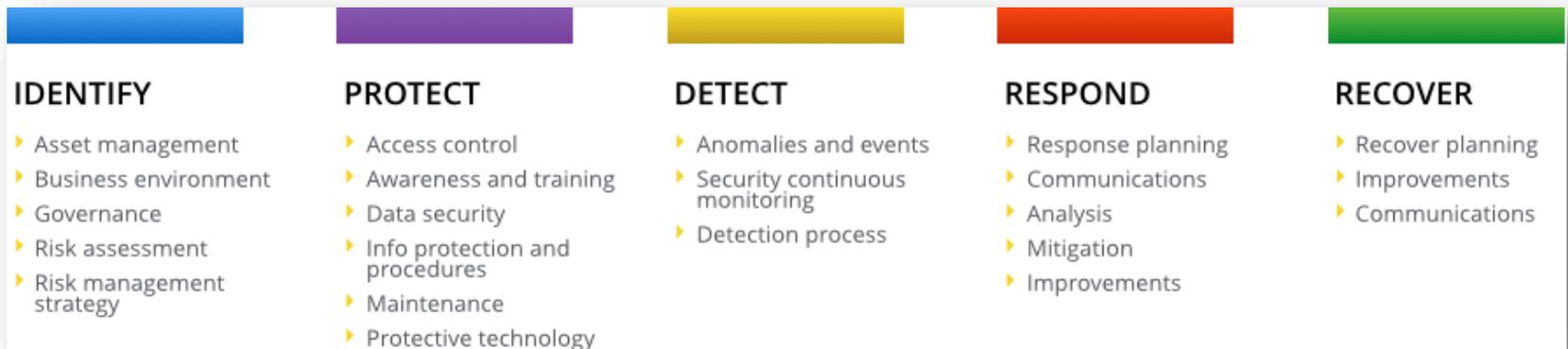


Cyber Security – Ihre Herausforderung



- › Neue Geschäftsanforderungen
 - › Kontinuierliche Veränderungen der Risikolage
 - › Steigende Sicherheits- und Compliance-Anforderungen
 - › Fehlende Ressourcen und Know-how
 - › Reduziertes Budget
 - › Verschiedene Partner, unterschiedliche SLAs
-

Etablierung einer Cyber Security Strategy



Quelle: www.nist.gov/cyberframework/

Identifizierung der unternehmenswichtigen Informationen

- › Wo befinden sich die Daten?
- › Wer benutzt sie?
- › Welchen Wert haben sie?
- › Wie sind sie derzeit geschützt?
- › Sind sie angreifbar?
- › Wenn ja, woran liegt das?

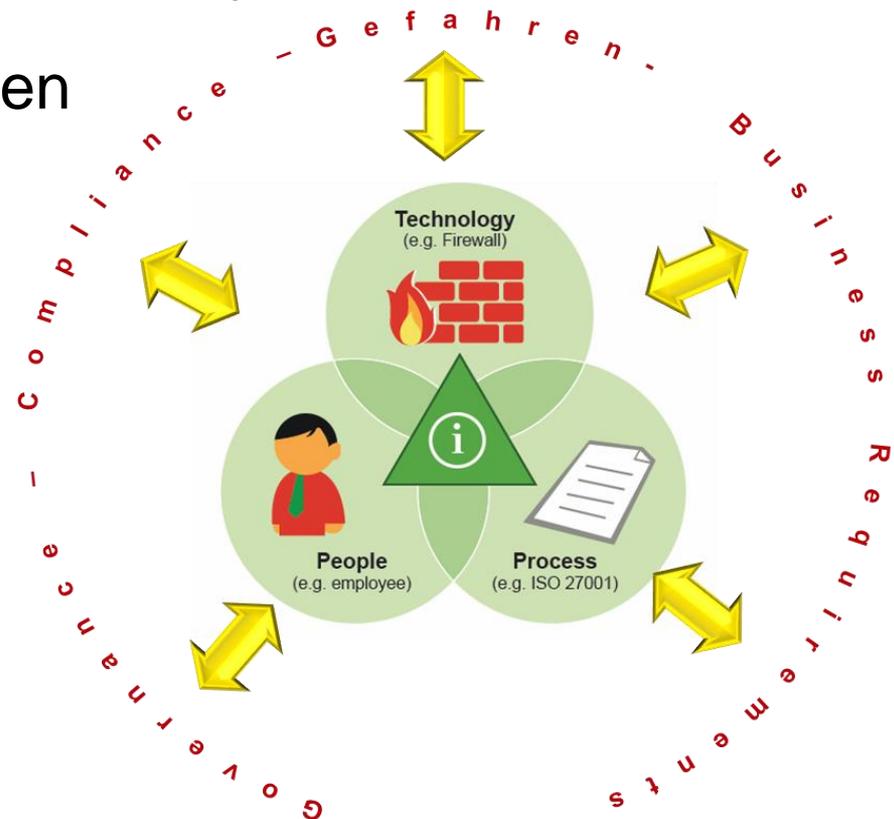


Leadership

› Implementation von Cyber Security

Massnahmen um die Folgen eines Cyber Angriffes zu begrenzen oder einzudämmen.

- › ISO 27002:2013
- › BSI Grundschutz
- › NIST Cyber Security Framework

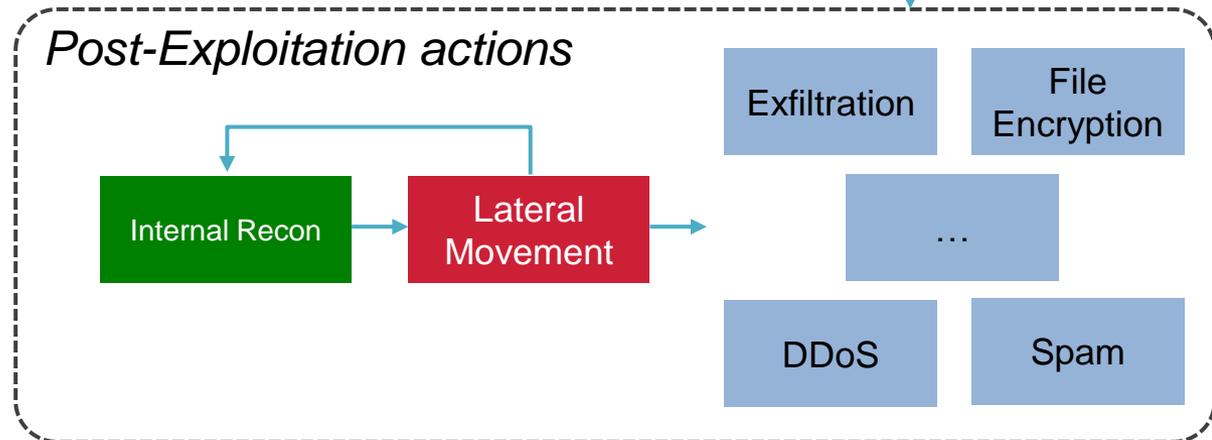


Detect and Respond InfoGuard Kill Chain

Targeted attack (SANS approach)



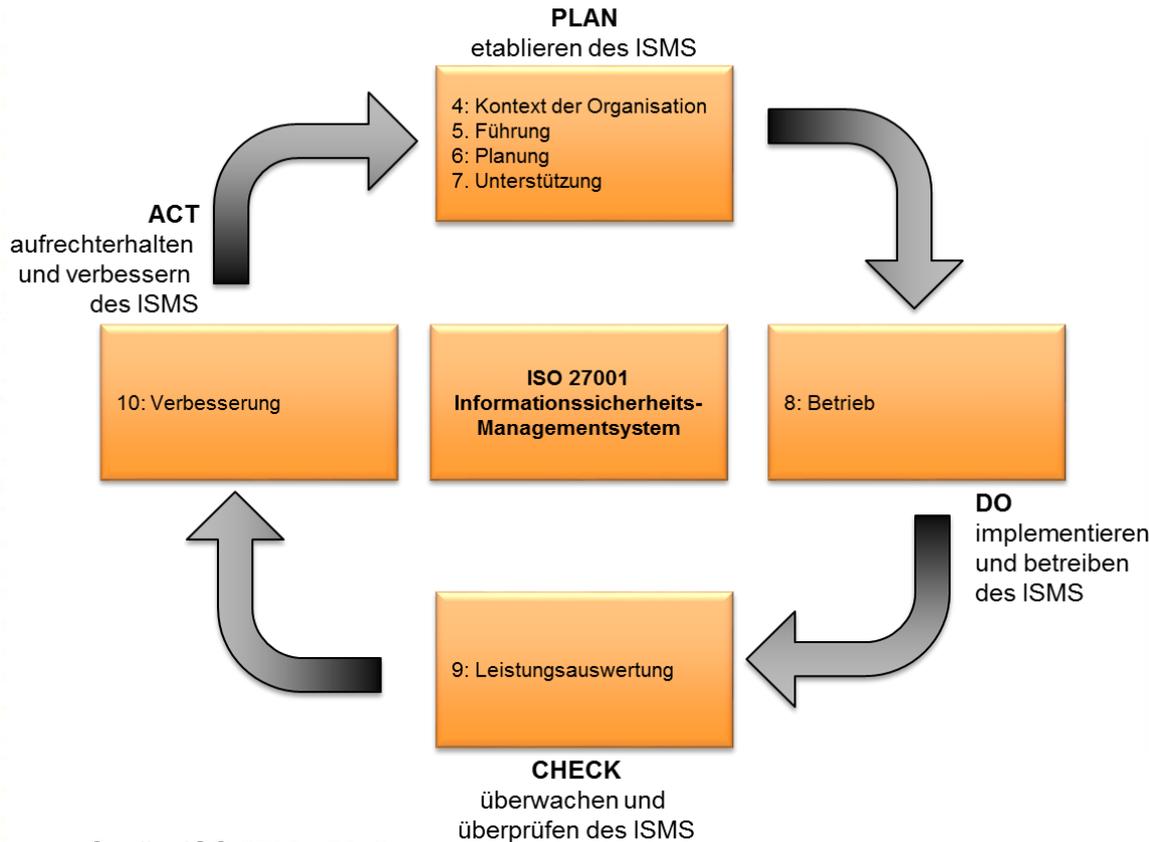
Opportunistic attack



Zum Teil ausgezeichnet von Gartner als „Cool Vendor in Security Intelligence“.

-
- › Unternehmen müssen in der Lage sein, ihre Mitarbeiter, Prozesse und Systeme so schnell wie möglich wieder arbeitsfähig zu machen.
 - › Eine effektive Schadensbehebung erfordert einen klaren und sorgfältig ausgearbeiteten Plan.

FAZIT



Quelle: ISO 27001:2013



Quelle: Symantec

Cyber-Resilience ist Ihr Rettungsschirm, wenn Ihre Cyber-Security versagen sollte.

FRAGEN?

