Studienprojekt 2020 – Cyber-Risiken

der Bundeswehr Universität München

Definition Cyber-Risiken

Das Cyber-Risiko ist eine **digitale Gefahr**, die von einer Person, Organisation oder einer Technologie bzw. einem Prozess initiiert wird, sich **zufällig oder mutwillig** durch ein **internes oder externes Ereignis** realisiert und in einer digitalen oder physikalischen **Beschädigung** von Daten, Dienstleistungen oder Produkten resultiert.

Kategorisierung von Cyber-Risiken

	Cyber-Risiken					
Ursache	Vorsätzliches Ereignis			Zufälliges Ereignis		
Bedrohungsart	**Hackerangriffe**	**Physische Angriffe**	**Informations-verbreitung**	**Menschliches Versagen**	**Technisches Versagen**	**Höhere Gewalt**
Angriffsform	- Malware - Phishing - Ransomware - DoS	- Physisches Eindringen in Unternehmensgebäude - Diebstahl vertraulicher Informationen	- E-Mail-Kampagnen - Boykottaufrufe über soziale Medien	- Programmierungsfehler - Verlust von Datenträgern - Versehentliches Veröffentlichen - Falsche Adressierung	- Hardwaredefekte - Softwarefehler	- Naturkatastrophen
Auswirkung	- Betriebsunterbrechung - Datenverlust - Datenschutzverletzung	- Datenverlust - Datenschutzverletzung	- Reputationsschaden - Datenschutzverletzung	- Betriebsunterbrechung - Datenverlust - Datenschutzverletzung	- Betriebsunterbrechung - Datenverlust	- Betriebsunterbrechung - Datenverlust

Deep Dive Hackerangriffe

MALWARE

Verletzung der Integrität des Systems oder der Daten mittels Schadsoftware/ Malware

→ Malware ist jede Art störender oder schädlicher Software, die ohne das Wissen des Benutzers auf ein Gerät zugreifen soll
→ Zu den Malware-Arten gehören u. a. Spyware, Phishing, Viren, Trojaner, Würmer und Ransomware

PHISHING

Datenschutzverletzungen und Ausspähen von Geschäftsgeheimnissen durch Phishing

→ Durch kompromittierte E-Mails mit gefährlichen Anhängen oder durch Nachahmung vertrauenswürdiger Websites stehlen Hacker persönliche Daten wie Passwörter, um so bspw. Zugriff auf gesamte Unternehmensnetzwerke zu erhalten

RANSOMWARE

Erpressung und Datenverluste durch Ransomware

→ Durch Ransomware (*dt. Lösegeld-Programme*) werden sensible Daten verschlüsselt und erst gegen Zahlung eines Lösegeldes wieder zugänglich gemacht. Die Wiederherstellung der Daten ist allerdings ungewiss, weshalb ein kompletter Datenverlust möglich ist

DOS

Unterbrechung der Verfügbarkeit von IT-Systemen oder Daten durch DoS-Angriffe

→ Denial of Service (*dt. Verweigerung des Dienstes*) – Folgen sind u. a. interne Betriebsunterbrechungen, Ausfall der Kommunikationswege mit Dritten und die Manipulation vernetzter Sicherheitsanlagen

Fallbeispiele

	WannaCry	NotPetya	Snowden
	Methode: Ransomware **Schadenhöhe**: mehrere Hundert Millionen Euro **200.000 Computer** in über **150 Ländern** **Betroffene:** Privathaushalte, Unternehmen, Infrastrukturbetreiber	**Methode:** Ransomware **Schadenhöhe:** über 10 Milliarden USD **Motiv:** Hackerangriff der russischen Regierung auf die Ukraine **Betroffene:** Privathaushalte, Unternehmen, Infrastrukturbetreiber	**Methode:** Physischer Datendiebstahl **Motiv:** Veröffentlichung von Geheimdienstpraktiken **Ziel:** NSA / GCHQ (Großbritannien)
Hintergründe	**Sicherheitslücke** im Betriebssystem Windows von Microsoft **Entwendung** von Eternalblue und **Veröffentlichung** bei „WikiLeaks“	**Zugang:** Sicherheitslücke im Betriebssystem Windows (u.a. Eternalblue)	**Zugang** zu vertraulichen Daten der Organisation sowie Sammlung von Informationen über Geheimdienstpraktiken
Ablauf	Ausbreitung des Virus nach Infektion eines Computers über dessen **Netzwerk** Aufforderung zur Lösegeldzahlung in Höhe von **300 Mio. USD** in Form von Bitcoins, um verschlüsselten Daten wieder entschlüsseln zu lassen	Daten werden **irreversibel verwürfelt**, Zahlung des geforderten **Lösegelds** führt zu nichts	**6. Juni 2013**: Veröffentlichung der Daten durch die „Washington Post“ und den „Guardian“
Learnings	**Technologieunternehmen** wie Microsoft → Sicherheitslücken schließen Cyber-Sicherheit auch als Verantwortlichkeit der **Privatpersonen** → Regelmäßige Updates	Problem des Hortens von Schwachstellen der **Regierungen** → **Sicherheitslücken** melden	**Überwachung** der Bürger durch Geheimorganisationen → **Sensibilisierung** bezüglich der eigenen Datensicherheit / Cyber-Sicherheit

Versicherungslösungen

	Privat	Selbstständige	Industrie
Art der Versicherung	- Als Zusatz zur Hausrat- oder Rechtsschutzversicherung - Separate Versicherung	- Stand Alone Police	- Zusatzbaustein über Property oder Financial Lines - Stand Alone Police
Versicherte Gefahren/Kosten (Auswahl)	- Ausgleich des finanziellen Verlustes durch Cyberattacken - Wiederherstellung von Daten	- Eigenschäden (Betriebsunterbrechung) - Drittschäden (Haftpflichtverletzungen)	- Betriebsausfall - Haftpflichtschäden aus Datenleaks
Zusätzliche Leistungen (Auswahl)	- Rechtsberatung zur Internetnutzung - IT-Assistance	- Training der Mitarbeiter - 24/7 Support - Datenforensische Untersuchungen	- Ausarbeitung eines Cyber-Konzepts mit IT-Sicherheitsexperten - Soforthilfe im Schadensfall - Ursachenermittlung

Universität der Bundeswehr München
Professur für Versicherungswirtschaft

Projektstudium WT/FT 2020
Laura Brobeil, Paul Büchting, Antong He, Marcel Heinrichsmeier, Maximilian Lang, Nadja Schlett