acomm

Vortragsabend Cybercrime

Stadtschloss Lichtenfels, 19.05.2022

Cyber-Security im Fokus

Agenda

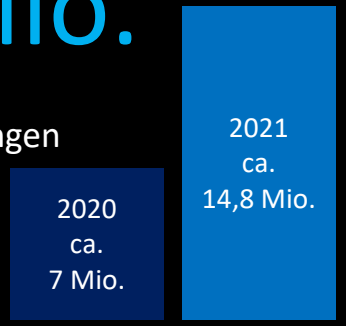
01 Die aktuelle Lage in Deutschland

02 Mögliche Angriffsszenarien

03 Basis für die Absicherung gegen Angriffe

Die aktuelle Lage in Deutschland 2021

14,8 Mio.
Übermittelte Schadensmeldungen

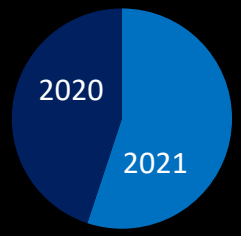


40.000
Täglich bis zu
BOT-INFEKTIONEN DEUTSCHER SYSTEME

44.000
Mails mit Schadprogrammen wurden in dt. Regierungsnetzen abgefangen.
2020 35.000

98%
aller geprüften Systeme waren durch Schwachstellen in MS Exchange verwundbar.

74.000
Webseiten wurden wegen enthaltener Schadprogramme durch Webfilter der Regierungsnetze gesperrt.
2020 52.000



144 Mio.
neue Schadprogramm-Varianten
+22%

14 Tage
Beträgt die durchschnittliche Totalausfallzeit nach einem Ransomware-Angriff

durchschnittlich **394.000** pro Tag
2020: 322.000

Höchstwert **553.000**
2020: 470.000

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

+360 % Daten-Leak-Seiten

Schweigegeld-Erpressung | Lösegeld-Erpressung | Schutzgeld-Erpressung

Mögliche Angriffsszenarien

01 PHISHING

Phishing oder Scam ist ein Social Engineering Angriff, bei dem versucht wird, die Zielperson zur Freigabe sensibler Informationen, wie Bank oder Kreditkartendaten zu bewegen.

02 CEO-FRAUD

CEO-Fraud gehört zu den Phishing-Angriffen, allerdings werden dabei gezielt Manager und Geschäftsführer unter Druck gesetzt um eine falsche Überweisung oder eine andere unerwünschte Aktion auszuführen.

03 BRUTE-FORCE / WÖRTERBUCH-ANGRIFF

Bei einem Brute-Force-Angriff wird ein "Ausprobieralgorithmus" verwendet um Anmeldedaten zu entschlüsseln. Daran angelehnt, wird bei einem Wörterbuch-Angriff versucht mit einer Wörterbuchliste aus gängigen Wörtern und Phrasen das Sicherheitssystem zu knacken.

04 MALWARE / RANSOMWARE

Als Malware-Angriff bezeichnet man allgemein Cyberangriffe mit Schadsoftware. Darunter fallen auch die sog. Ransomware-Angriffe oder Verschlüsselungstrojaner. Diese haben das Hauptziel Daten abzufischen und Lösegelder zu erpressen.

04 DDOS / DOS

Ein Denial-of-Service-Angriff zielt darauf ab, ein Netzwerk oder Ressourcen zu blockieren, indem ein Ziel mit künstlichem Datenverkehr überflutet wird. Ziel ist eine Störung oder Unterbrechung des Geshäftsbetriebes bzw. die Erpressung von Lösegeldern.

Weitere Angriffsmöglichkeiten

SQL Injection

Cross-Site-Scripting

Man-in-the-Middle

Social-Engineering

Spoofing

Basis für die Absicherung gegen Angriffe

Cyber-Security Mythen

Wir haben EINEN Penetration-Test durchgeführt.

Wir wurden noch NIE angegriffen. Unser Sicherheitssystem ist also gut.

Wir haben eine Firewall.

Wir richten uns nach Industriestandards und Best-Practice-Beispielen.

Wir haben in strenge Sicherheitskontrollen investiert.

Die Sicherheit wird ausreichend durch das IT-Team geleitet.

Wir müssen nur unsere Anwendungen mit Internetzugriff absichern.

Wir haben unser IT-Sicherheits-Projekt fertiggestellt.

Wir sind statistisch gesehen nicht gefährdet und für uns interessiert sich sowieso niemand.

Basis für die Absicherung gegen Angriffe

Unternehmenssicherheit &
IT-Sicherheit

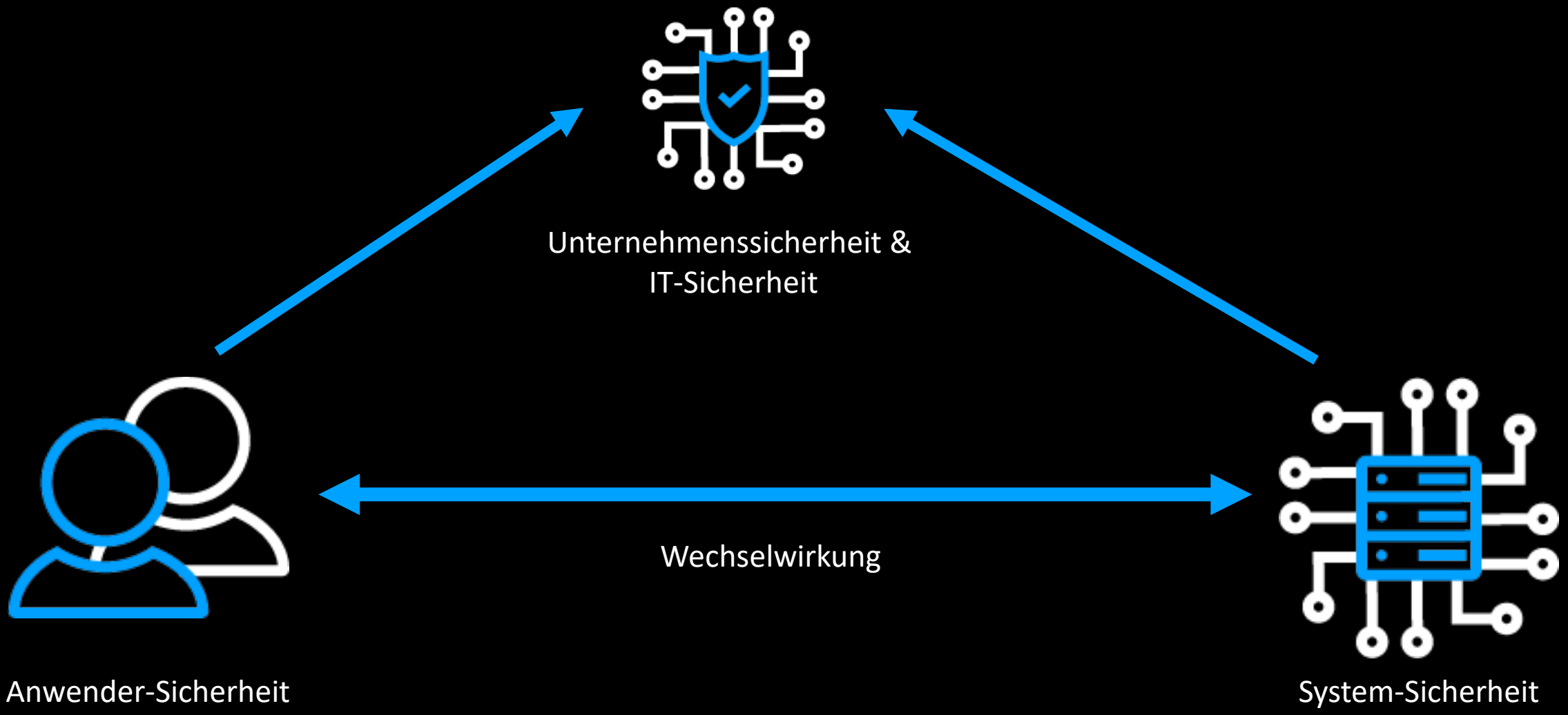
IT-Sicherheit

Spannungsfeld

VS.

Unternehmensziele

Basis für die Absicherung gegen Angriffe



Basis für die Absicherung gegen Angriffe

Anwender-Sicherheit / Mitarbeiter-Awareness

Starke Passwörter

Passwörter nicht auf Notizzetteln notieren

PCs Sperren

Räume abschließen

Basis für die Absicherung gegen Angriffe

Anwender-Sicherheit / Mitarbeiter-Awareness

Links in E-Mails genau prüfen

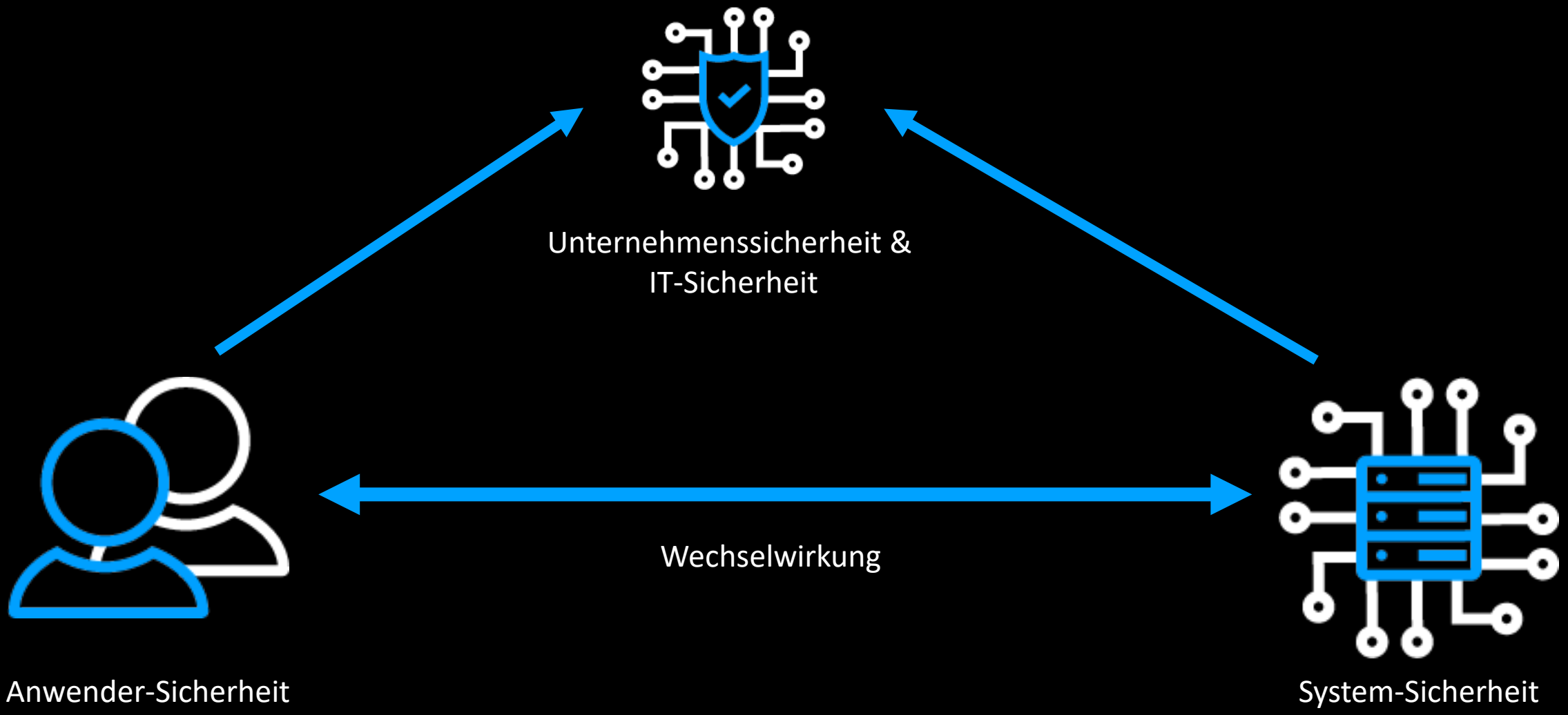
Absender von E-Mails genau prüfen

Notfallplan

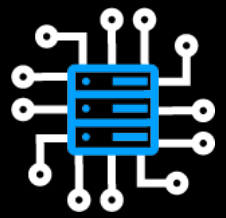
Aktuelle & vollständige IT-Dokumentation

Awareness-Training für Mitarbeiter

Basis für die Absicherung gegen Angriffe



Basis für die Absicherung gegen Angriffe



IT-Systemsicherheit

Passwortrichtlinie & starke Passwörter systemseitig erzwingen

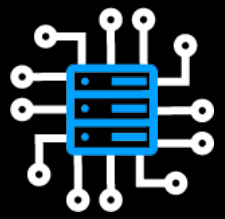
Eindeutige Benutzerkennungen für jeden Benutzer

Berechtigungskonzept | Benutzerrollen | Gruppenrichtlinien

Aktueller & vollständiger Notfallplan

Aktuelle & vollständige IT-Dokumentation inkl. Inventarisierung und Benutzerzuordnung

Basis für die Absicherung gegen Angriffe



IT-Systemsicherheit

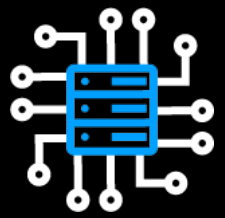
Engmaschige BackUps & BackUp-Konzept inkl. Datensicherungskontrolle und Wiederherstellungstests

Firewall und Virenschutz

Installation von Updates und Sicherheitsaktualisierungen

Aktuelle Hard- und Software

Basis für die Absicherung gegen Angriffe



IT-Systemsicherheit

Netzwerksegmentierung

Passwortmanager

Einsatz eines zentralen Netzwerk-Management-Systems

IT-Sicherheitsaudit

acomm GmbH
Bischof-von-Dinkel-Str. 12
96231 Bad Staffelstein

Tel +49 (0)9573 25320-0
Mail info@acomm.de
Web www.acomm.de