Sichere Digitalisierung – Rezepte für die erfolgreiche Umsetzung

biners security solutions

biners

Optimizing business information security – efficiently

Sichere Digitalisierung – Rezepte für die erfolgreiche Umsetzung

Agenda

- Die Digitalisierung ist in vollem Gange
- Cyberattacken – beliebte Angriffsformen
- Cybervorfälle – aktuelle Beispiele
- Cyberkriminalität – Der Weg des geringsten Widerstands
- Stand der Sicherheit bei Unternehmen bis 500 Mitarbeiter
- Nachhaltig das Geschäft absichern
- Rezepte in einigen Bereichen
- Zu guter letzt …

Die Digitalisierung ist weit fortgeschritten …

... sowohl bei den Konsumenten als auch in der Industrie

Cyberattacken – beliebte Angriffsformen

Typische Angriffsformen – die auch kombiniert werden

- **Malware-Angriffe** = schadhafte Software/Programme: kann auf einem Computer nahezu alles von Datendiebstahl bis hin zur Verschlüsselung gegen Lösegeld
- **Phishing emails** = schadhafte Emails: Computernutzer sollen Zugangsdaten, Passwörter herausgeben oder eine schadhafte Aktion ausführen (zB. Herunterladen von Malware)
- **Denial of Service attacks** = Computerausfall provozieren: es werden typischerweise Web-Server (zB. Onlinemarktplatz) durch Massenangriffe lahmgelegt
- **Man in the middle attacks** = ein Schad-Computer klemmt sich ein: typischerweise unbemerkt von den Kommunikationspartnern werden kritische Informationen gestohlen oder schadhafte Transaktionen ausgeführt.

Cybervorfälle – aktuelle Beispiele

Es sind global große Schäden in allen Wirtschaftszweigen vorhanden

Ursache = Malware (Verschlüsselungstrojaner)

Ca. 300 Mio. USD Schaden durch Cybervorfall

Großangelegte Cyberattacke: Hacker legen weltweit Firmen lahm

Dienstag, 27.06.2017 20:13 Uhr

Per Erpressersoftware haben Hacker den Betrieb von Flughäfen, Frachtschiffen und Banken massiv gestört. Die größte Containerreederei der Welt Maersk meldete globale IT-Ausfälle, auch deutsche Firmen sind betroffen.

http://www.spiegel.de/netzwelt/web/maersk-hacker-legen-computer-von-groesster-reederei-der-welt-lahm-a-1154696.html

Cybervorfälle – aktuelle Beispiele

Lösegeldforderungen sind stark auf dem Vormarsch, jedoch sind diese nur ein Teil des Gesamtschadens.

DDoS-Attacke mit Lösegeld

Mittleres Unternehmen (50-250 Mitarbeiter)

Ausfall eines kritischen Webservers für 4 Stunden. Ca. 48 Stunden über das Wochenende Zeit, Lösegeld in Bitcoins (Internetwährung) zu zahlen.

Ursache: Distributed-Denial-of-Service-Attacke auf einen erfolgskritischen Webserver (Initialattacke zum Beweis der Fähigkeit)

Aufwand:

- Externer Cybersicherheitsberater
- Zusatzkosten Data Center-Betreiber
- Externe Rechtsberatung (Anzeige LKA)
- Zusatzkosten Personaleinsatz IT am Wochenende (Vorbereitung Notbetrieb, Kundenkommunikation)

Ransomware (Verschlüsselung & Lösegeld)

Kleinunternehmen (<20 Mitarbeiter)

Verschlüsselung aller Arbeitsplatzrechner und Server. Warenwirtschaft und Auftragsdisposition ca. 2 Wochen nicht verfügbar. Danach Notbetrieb mit effektivem Datenverlust von 4 Wochen.

Ursache: Schadhafter Emailanhang mit Verschlüsselungstrojaner

Aufwand:

- Externer Cybersicherheitsberater
- Externer IT-Forensiker
- Externer IT Betreiber (Aufbau Notbetrieb)

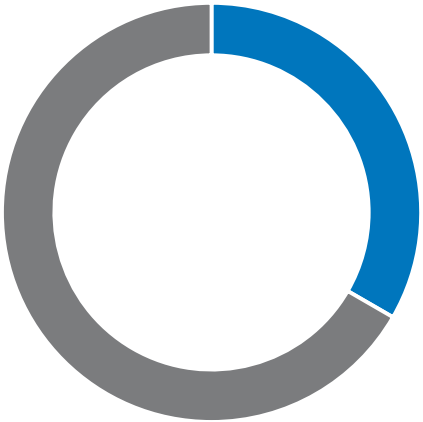
Der Weg des geringsten Widerstands

Cyberkriminelle nutzen die einfachsten Wege um Geschäft zu machen

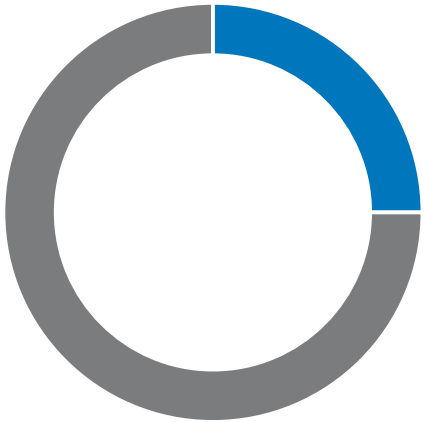
Stand der Sicherheit bei KMU

Unternehmen bis zu 500 Mitarbeiter – Basissicherheit ist weiterhin zu optimieren

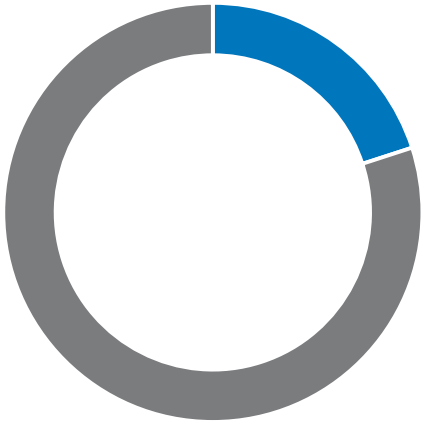
Datensicherung



Firewall



Virenscanner



https://www.versicherungsbote.de/id/4861018/Cyberversicherung-KMU-Versicherungsschutz/#comments

Nachhaltig das Geschäft absichern

Mit überschaubarem Zeitaufwand und Finanzmitteln kann das individuelle Cybersicherheitsniveau schnell auf über 80% gebracht werden.

Empfehlung: alle 3 Sicherheitskategorien vernetzt angehen.

Organisatorische Sicherheit

1. "**Kronjuwelen**" sowie **kritische Geschäftsabläufe** definieren und **potenzielle Schäden** durch Cybervorfälle einschätzen
2. **Krisen-**, **Notfall-** und **Wiederanlaufplan** aufstellen und üben
3. **Sicherungskopien** von wichtigen Geschäftsinformationen/-verträgen anfertigen sowie **Backups** von Daten/Konfigurationen für den technischen Notbetrieb sicherstellen
4. Definition der **(Cyber-)Sicherheitsvorgaben** und Kommunikation (intern/extern)

Menschliche Sicherheit

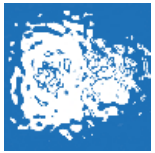
1. Kontinuierliches **Awareness-Training** aktueller Angriffs-szenarien für interne und externe Mitarbeiter (zB. Phishing, CEO-Fraud, Social Engineering)
2. **4-Augen-Prinzip** für erfolgskritische Genehmigungsprozesse
3. **Nutzerschulungen** zur sicheren Nutzung von IT-Systemen (u.a. sichere Passwörter)

Technische Sicherheit

1. **Aktuelles Inventar** der genutzten Endgeräte, Server, Netzwerkgeräte und Software (auch nicht-authorisierte)
2. **Sichere Konfigurationen** für Hardware und Software auf Endgeräten (Laptops, Workstations, Smartphones), Servern und Netzwerkgeräten inkl. Basis-Sicherheit
3. **Kontinuierliche Updates** der Hard- und Software sowie aktive Steuerung der Verwundbarkeiten/ Sicherheits-lücken
4. **Limitierung** der **Admin-Rechte** und striktes 4-Augenprinzip für IT Administratoren

Rezepte

Schutz des Emailsystems



Cyberattacke

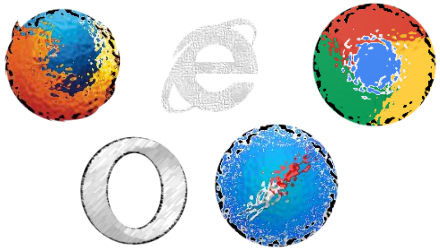
- **Malware** = schadhafte Software/Programme: kann auf einem Computer nahezu alles von Datendiebstahl bis hin zur Verschlüsselung gegen Lösegeld
- **Phishing emails** = schadhafte Emails: Computernutzer sollen Zugangsdaten, Passwörter herausgeben oder eine schadhafte Aktion ausführen (zB. Herunterladen von Malware)

Schutzmaßnahmen

- Erhöhung der Aufmerksamkeit der Mitarbeiter/Dienstleister
- (Teil-)Blockade von Email-Anhängen (zB. MS-Office Dateien und pdf-Dokumente)
- Blockade von ausführbaren Dateien/Programmen (Makros, exe-Dateien, Skripte)
- Blockade von Links aus Emails in das Internet
- Freigabe von definierten Internetseiten bzw. Sperre von ungewollten Internetseiten
- …

Rezepte

Sicheres Surfen und Software-Downloads im Internet



Cyberattacke

- **Malware** = schadhafte Software/Programme: kann auf einem Computer nahezu alles von Datendiebstahl bis hin zur Verschlüsselung gegen Lösegeld
- **Phishing emails** = schadhafte Emails: Computernutzer sollen Zugangsdaten, Passwörter herausgeben oder eine schadhafte Aktion ausführen (zB. Herunterladen von Malware)

Schutzmaßnahmen

Internetbrowser / lokale Computer werden zentral verwaltet und stark reglementiert:

- Pop-Up Blocker, Adware Blocker
- Automatisierte Cookie / Surf-Historienlöschung nach Schließung des Browsers
- Zentrale Softwareverteilung – keine lokale Installationen
- Internetzugriff über Zwischencomputer (Proxy)
- Sperrung von Internetseiten
- …

Rezepte

Sichere Kommunikation an öffentlichen Hotspots oder Hotel-WLAN

Cyberattacke

- **Man in the middle attacks** = ein Schad-Computer klemmt sich ein: typischerweise unbemerkt von den Kommunikationspartnern werden kritische Informationen gestohlen oder schadhafte Transaktionen ausgeführt.

Schutzmaßnahmen

- Blockade von öffentlichen Hotspots
- Verschlüsselte Kommunikation wird im Minimum erzwungen / unbekannte Schlüssel werden nicht akzeptiert
- Sichere Verbindung wird erzwungen (zB. VPN)
- …

Rezepte

Sichere Geschäftsanwendungen / Webseiten im Internet

Cyberattacke

- **Denial of Service attacks** = Computerausfall provozieren: es werden typischerweise Web-Server (zB. Onlinemarktplatz) durch Massenangriffe lahmgelegt

*Open Web Application Security Project-owasp.org

Schutzmaßnahmen

- Betreiben der Webseite(n) in professionellem Rechenzentrum
- Mindestverfügbarkeitszeit des Webservers auch für Cyberattacken
- Klärung spezieller Schutzmaßnahmen (DDoS Protection) und entsprechender Servicekosten
- Datenwiederherstellung definieren
- Laufende Härtung der Shopsoftware/ Anwendung im Internet nach OWASP*-Grundsätzen
- Regelmäßige Schwachstellenanalyse durch simulierte Hackerangriffe (Pen-Tests)
- …

Rezepte

Sichere Speicherung im Internet

Cyberattacke

- **Man in the middle attacks** = ein Schad-Computer klemmt sich ein: typischerweise unbemerkt von den Kommunikationspartnern werden kritische Informationen gestohlen oder schadhafte Transaktionen ausgeführt.

Schutzmaßnahmen

- Besonders kritische Daten in speziell gesicherten Lösungen speichern
- Bei Nutzung von etablierten Massen-Cloud-Speicherdiensten Verschlüsselung der Daten realisieren
- Verschlüsselte Kommunikation bei der Datenübertragung sicherstellen
- …

*Open Web Application Security Project-owasp.org

Zu guter letzt ...

Vielen Dank!

biners – business information security
biners Deutschland GmbH
Denglerstr. 25
53173 Bonn
T: 0228 4097 3250
E: info@biners.eu
W: www.biners.eu

Sicherheit im Team erzeugen

Bindet interne sowie externe Partner ein und nutzt das Know-How von Profis.

10 Empfehlungen für das Management

1. Seid vorbereitet, noch seid Ihr davongekommen!
2. Setzt auf Früherkennung und permanente Bekämpfung
3. Nutzt „managed“ Securitysolutions von Profis
4. Nehmt staatliche Meldepflichten ernst
5. Schult Beschäftigte, Partner und Dienstleister
6. Überprüft sicherheitsrelevante Geschäftspartner/Mitarbeiter
7. Verschlüsselt Daten und Datenkommunikation
8. „Managed“ aktiv die Daten, vor allem Backups
9. Haltet Systeme und Software aktuell
10. Stellt einen Notfall- und Anlaufplan auf und übt diesen

10 Empfehlungen für Mitarbeiter

1. Lasst Euch nicht „Phishen“ – betrügerische Emails können zumeist schnell erkannt werden
2. Betriebsinternas sind Internas - äußert Euch mit Bedacht in sozialen Medien
3. Nutzt niemals Euer Firmenemailkonto und Firmenpasswort, um Euch bei Internetdiensten zu registrieren
4. Seid freundlich aber nicht sofort zutraulich – Social Engineers suchen einfache Zugangswege
5. Nutzt sichere Passwörter und erneuert diese regelmäßig – bitte niemals das Passwort weitergeben oder an den Bildschirm kleben
6. Seid besonders vorsichtig bei der Nutzung mobiler Endgeräte, wenn Ihr auf Firmendaten zugreift – es sind alle Mitlesetools zu deaktivieren
7. Nutzt keine öffentlichen Hotspots (zB. in Hotels, Bahn, Flughäfen), wenn Ihr auf Firmendaten zugreift – außer ihr nutzt einen sicheren, verschlüsselten Kanal.
8. Geht sorgfältig mit mobilen Datenspeichern um. Wichtige Daten sind zu verschlüsseln. Geschenkte USB Sticks dürfen nicht mit Firmenrechnern genutzt werden
9. Schließt wichtige Dokumente ein – auch bei kurzfristiger Abwesenheit
10. Seid vorsichtig in der Weitergabe von Dokumenten – vertrauliche Dokumente sind vertraulich

EU-Datenschutz

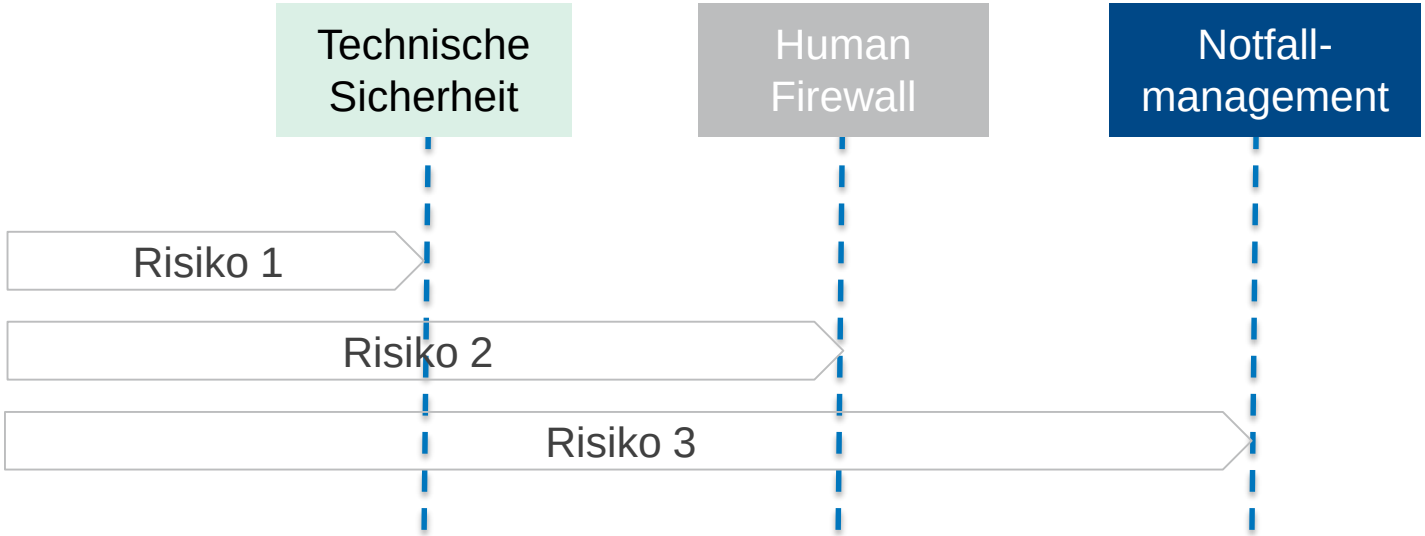
Technische und organsatorische Sicherheit sind integraler Bestandteil

Signifikante Bußgelder

Bis zu 4% des weltweiten Umsatzes bzw. 20 Mio. €

Verteidigungslinien der Unternehmen

IT/Technik als erste Verteidigungslinie und die Human-Firewall als letzte Hürde – danach kommt nur noch Notfallmanagement



Es beginnt zumeist mit einer Email

eMails – Fluch und Segen, aber ohne geht es (noch) nicht

Chefmasche, CEO-Fraud

Enorme Zuwächse der Schäden

Chefmasche …

… verursacht große Schäden und geht zumeist auf Phishing Emails zurück

2013-2017 >5 Mrd. USD weltweit

Gegenmaßnahmen

- 4-Augen-Prinzip
- Erhöhung der Aufmerksamkeit vor allem im Finanzbereich
- Limitierung der Verfügungsberechtigung über Bankkonten
- Stellvertreterregelung
- …