IT-Sicherheit

Gerade in Corona-Zeiten, wo immer mehr Mitarbeiter über Remote-Verbindung von zu Hause aus auf sensible Unternehmens- und Kundendaten zugreifen, ist es wichtig, auf eine funktionierende IT-Sicherheit zurückgreifen zu können. Wenn Mitarbeiter lernen, wie sie Cyberbedrohungen erkennen und was die ersten Maßnahmen zum Schutz der Daten sind ist die größte Sicherheitslücke in Ihrem System geschlossen. Auch Hacker werden immer raffinierter. Die alt-bewährten Prüf-Methoden bei Phishing-Mails mit dem Check der Ansprache, Rechtschreibfehler oder dem Absender sind heute nur noch bedingt zielführend. Heutzutage sehen Phishing-Mails dem Original so ähnlich, dass erst beim genaueren Hinsehen Auffälligkeiten sichtbar werden. Eine durchgängige Sicherheitsstrategie und die passende Security-Software können hier allerdings helfen.

In diesem Beitrag beleuchten wir, was IT-Sicherheit für Unternehmen bedeutet, welche Arten der Cyberkriminalität es gibt und welche Möglichkeiten, Anforderungen und Besonderheiten zu beachten sind um die die eigene IT sicherer zu machen.
Die Unterlage ist so aufgebaut, dass diese auch direkt als Mitarbeiter-Information verwendet werden kann.

Ansprechpartner

Angelina Schock
Managing Partner – GCS Consulting GmbH
E-Mail: schock@gcs-consulting.de
Telefon: +49 89 89136516

Bildquelle:saffroninteractive.com

IT-Sicherheit

Aktuelle Situation

„Ein Unternehmen, dass noch **keinen Cyberangriff** verzeichnet hat, ist entweder nicht interessant genug oder es hat den Angriff einfach nur nicht bemerkt.“ – Sprecher BSI[2]

87.106 Fälle von Cybercrime im engeren Sinn (2018)[1]

22.051 Tatverdächtige von Cybercrime-Delikten[3]

69% versuchen, Benutzer zu einer schädlichen URL zu verleiten. 31% versuchen über böswillige Anhänge Schaden zu zufügen[4]

3 von 4 Unternehmen wurden Opfer von Sabotage, Datendiebstahl oder Spionage[5]

Word, PowerPoint und Excel sind die am häufigsten vorkommenden schädlichen Datei-erweiterungen[6]

Der Informations-verlust macht 43% der Kosten bei Cyberangriffen aus[7]

Datenschutz-verletzungen dauern in der Regel mehr als 6 Monate, bis sie bemerkt werden[8]

Digitale Angriffe haben bei 7 von 10 Unternehmen Schäden verursacht[9]

Insgesamt über 100 Mrd. Euro Schaden pro Jahr[10]

Quellen: [1] BKA | [2] Sprecher BSI | [3] BKA | [4] f-Secure | [5] Bitkom | [6] Cisco | [7] accenture | [8] Cisco | [9] Bitkom | [10] Bitkom

Phishing
Abgreifen von relevanten Zugangsdaten (Banken, PayPal, Amazon etc.)

Malware
Verschiedenste Schadsoftware (Jscript, Makros, Java), Ziel ist Remote Access und Nutzung von Ressourcen für Angriffe bzw. Ausspähen von sensiblen Daten

Ransomware
Verschlüsselung von Daten mit anschließender Erpressung zur Entschlüsselung via Bitcoin Zahlung

Social Engineering
Zwischenmenschliche Beeinflussung mit dem Ziel bei Personen Verhaltensweisen hervorzurufen (z.B. Vertrauliche Informationen)

Trojaner
Platzierung von Schadsoftware mit der Möglichkeit der Fernsteuerung

Denial of Service
Überlastung eines Internetdienstes mithilfe einer Vielzahl gezielten Anfragen

CEO Fraud
Gefälschte E-Mail von Mitglied der Unternehmens-führung mit dringender Zahlungsaufforderung

Besteller Betrug/ Fake Identity
Bestellung auf Rechnung mit abweichender Lieferadresse, Rechnung geht an Betrogenen

Bitcoin Mining
Schürfen von Bitcoins ohne Wissen des Nutzers

Die wichtigsten Betrugsformen im Überblick:

- Phishing
- Malware
- Ransomware
- Social Engineering
- Trojaner
- Denial of Service
- CEO Fraud
- Besteller Betrug/Fake Identity
- Bitcoin Mining

Beispiele von Gefahren:

Verfügbarkeit:
- Festplattencrash im Fileserver
- Backup lässt sich nicht wiederherstellen
- Kollege startet einen Trojaner aus einem Mailanhang – alle Zugriffe gesperrt

Vertraulichkeit:
- Mail geht versehentlich an falschen Empfänger
- USB-Stick mit Kunden-Daten geht verloren
- Kollege verrät nach Social Engineering ein Passwort

Integrität:
- Software speichert wegen eines Fehlers falsche Daten
- Kollege löscht aus Versehen Teile von Daten

Authentizität:
- „Nigerianischer Prinz“ will Ihnen Geld schenken
- Passwort auf gefälschter Paypal-Seite eingegeben
- Betrüger gibt sich als Chef aus und lässt sich Geld überweisen

Was bedeutet „IT-Sicherheit“?

Verfügbarkeit	Vertraulichkeit
Daten müssen zu jeder Zeit in geeigneter Form zur Verfügung stehen.	Daten dürfen nur von Personen verändert oder eingesehen werden, die auch berechtigt sind
Integrität	**Authentizität**
Daten dürfen nicht unerkannt bzw. unbemerkt verändert werden.	Daten müssen jederzeit ihrem Ursprung zugeordnet werden können.

Bewusstsein schaffen

Cyberangriffe können sowohl gezielt auf Ihre Firma oder einen einzelnen Mitarbeiter, als auch unspezifisch zum Beispiel via Malware per E-Mail-Anhang erfolgen.

Mitarbeiter wissen oft gar nicht wo Gefahren lauern können. Deswegen ist es wichtig, Informationen über mögliche Cyberangriffe zur Verfügung zu stellen. Unachtsamkeit der Mitarbeiter und die damit zusammenhängende Nichterkennung erster Anzeichen ist in den meisten Fällen die Ursache von Cyberkriminalität.

Gezielter Angriff oder Zufall?

- **Spezifische Angriffe**

- Gezielt auf ihr Unternehmen
- Zuvor definiertes Ziel
- Mehrere Wochen bis Monate Vorbereitungszeit
- Informationen über das Ziel werden mittels Social Engeneering gesammelt
- Gewohnheiten werden ausgenutzt (z.B. CEO Fraud)
- Oft arbeiten mehrere Menschen zusammen um Vertrauen zu erwecken

- **Unspezifische Angriffe**

- Kriminelles Grundrauschen des Internets
- Massenware (wahllose Empfänger)
- Meist auffällige Fehler in Orthographie, jedoch auch perfekte Exemplare
- Antivirenprogramme in den ersten Tagen „blind“
- Links in Mails verweisen auf ähnliche Domains (kleine Abänderungen in der URL z.B. amazon.con oder Paypol.com)
- Mehrstufige Angriffe (z.B. Makro im Wordanhang – lädt Java Script aus dem Internet – dieses lädt Schadsoftware – lädt weitere Teile)

Passwort-Manager
- Rollenmodell mit Unternehmens- und Verantwortungsstruktur für differenzierten Datenzugriff

Security Software
- Intelligente und lernfähige Software zur Absicherung und effektiven Verwaltung sensibler Unternehmens- und Kundendaten inkl. Back-Up-Methodik
- Patch-Management
- Permanentes Monitoring inkl. Benachrichtigung kritischer Infrastruktur
- Gateway-Lösungen für eigenen Mailserver, Implementierung von Gateway-Appliances für das Mail Handling
- Newsletter des BSI [1] abonnieren

Mitarbeiterschulungen
- Sensibilisierung und Schulung von Mitarbeitern auf allen Hierarchieebenen bezüglich der tatsächlichen Angriffsszenarien
- Zentrale Guidelines bereitstellen
- Plausibilitätskontrolle bei Anrufen / E-Mails

Meldeketten und Notfall-Szenario
- Fragwürdige oder verdächtige Aktionen müssen gemeldet werden
- Frühe Einleitung von Gegenmaßnahmen tragen erheblich zur Schadensbegrenzung bei
- Desaster Recovery Plan entwickeln, solange die Infrastruktur noch funktional ist
- Simulation eines Worst Case Szenarios im Sinne einer Feueralarm-Übung

Prävention ist günstiger als reagieren

Maßnahmen

Passwort-Manager

Unternehmensweit standardisierte Security-Software

Mitarbeiterschulungen

Meldeketten und Notfall-Szenarien etablieren

[1] Bundesamt für Sicherheit und Informationstechnik

Fazit

Es kann jeden treffen

Cyberkriminalität ist mittlerweile in der Mitte der Gesellschaft angekommen. Auch wenn die Fallzahlen zur Cyberkriminalität stetig steigen und die komplexen Bedrohungen immer größer werden ist mit einfachen Maßnahmen schon ein wichtiger Schritt zu einer effektiven IT Sicherheit möglich. Hier hilft am besten Prävention zum Beispiel in Form moderner IT-Security Lösungen aber auch von Awareness Trainings der Mitarbeiter. Gerade Trainings und die Bereitstellung von Informations-material für Mitarbeiter sollten nicht unterschätzt werden, da 30% der sicherheitskritischen Vorfälle auf menschliches Versagen zurückzuführen ist.[1] . Jeder kann zum Opfer werden. Aus diesem Grund sollte auch jeder, der sich online bewegt, geeignete Schutzmaßnahmen ergreifen.

7 Punkte für eine sichere IT

- Software zur Absicherung und effektiven Verwaltung sensibler Unternehmens- und Kundendaten
- IT-Systeme, mobile Geräte und Dienste stets Updaten
- Erstellung gut verständlicher Sicherheitsrichtlinien
- Berechtigungskonzept inkl. Zugriffsbefugnisse
- Regelmäßige Back-ups inkl. Desaster Recovery Plan mit Worst-Case Szenario Trainings
- Absicherung externer Kommunikation über VPN-Technik
- Regelmäßige Schulungen der Mitarbeiter für das Thema IT-Sicherheit

[1] Quelle: Kaspersky

KONTAKT

… wir freuen uns auf Ihre Anfrage:

Anschrift
GCS Consulting GmbH
Frankfurter Ring 193a
80807 München

Fon +49 89 891365 -0 **Fax** +49 89 891365 -29

E-Mail info@gcs-consulting.de
Website www.gcs-consulting.de

Angelina M. Schock | Managing Partner
schock@gcs-consulting.de | +49 151 14051819

Niklas Reischmann | Junior Consultant
reischmann@gcs-consulting.de | +49 89 89136522