Klickkomplizen

auf einen klick

Schutz vor Cyberkriminalität

INTRO

Das Thema Cyberkriminalität und Hacking wird zunehmend relevanter für uns, egal ob Privatperson, Mitarbeiter:in oder Geschäftsführer:in.

Kann ich mein Unternehmen vor Hackerangriffen schützen? Nein, zumindest nicht zu 100 %. Cyberangriffe werden zukünftig laut Prognosen häufiger auch kleine und mittelständische Unternehmen treffen. Wir stellen euch die gängigen Methoden vor, wie man sie erkennt und geben zahlreiche Tipps für Schutzmaßnahmen.

ARTEN VON CYBERANGRIFFEN

Cyberangriffe ARTEN

RANSOMWARE (Erpressungssoftware)

Verschlüsslungstrojaner, mit welchem die Hacker die Eigentümer:innen aus ihrem eigenen Gerät, den dort liegenden Daten o.ä aussperren. Erpressung von Lösegeld mit der Drohung, die Daten zu veröffentlichen oder zu löschen.

häufigste Art der Cyberangriffe

PHISHING

Versand gefälschter E-Mails, SMS, Links etc. um an die Daten des Users zu kommen. ACHTUNG: Auch QR-Codes können dem Phishing dienen.

DDOS-ATTACKEN*

Attackieren des Servers eines Unternehmens mit extrem vielen Anfragen, sodass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht. Die Angreifer:innen sind schwer zu ermitteln.

* Distributed Denial-of-Service

MAN-IN-THE-MIDDLE-ANGRIFF

Person schleicht sich unbemerkt in Kommunikation zweier oder mehrerer Personen ein und liest Informationen mit oder manipuliert diese.

BRUTE-FORCE-METHODE

Ausrechnen und Erraten von Passwörtern, indem in extrem kurzer Zeit diverse Zeichenkombinationen ausprobiert werden.

ADVANCED PERSISTENT THREAT

Ein:e ausgebildete:r, typischerweise staatlich gesteuerte:r Angreifende:r hackt sich in ein System oder Netz, späht Daten aus, manipuliert Informationen etc. zum Zweck der Spionage.

Für die Geschädigten bedeuten die Angriffe u.a. Betriebsstörungen, Umsatzeinbußen, Kosten für Datenwiederherstellung bis hin zu vollständiger Sabotage und dem Auslöschen des Unternehmens oder dem Abschalten ganzer Netze.

SCHWACHSTELLEN

Welche Schwachstellen nutzen die Angreifenden?

- **Schwache oder leicht zu erratende Passwörter**
- **Mehrfaches Verwenden eines Passwortes für verschiedene Websites**
- **Einloggen mit Dienstlaptop auf privat genutzten Websites**
- **Nutzung des privaten Smartphones für Unternehmenszwecke**
- **Informationen, welche über das Unternehmen oder die Privatpersonen im Internet zu finden sind**
- **Sicherheitslücken in Software + Netzwerken**

SCHUTZMASSNAHMEN

Wie kann man sich (zum Teil) vor solchen Angriffen schützen?

- Passwörter regelmäßig ändern, kompliziert und lang halten
- Schulungen für Geschäftsführende und Mitarbeitende besuchen
- bei jedem Tool, Website oder Account ein anderes Passwort wählen
- Anzahl der Admins von Seiten und Tools möglichst gering halten
- Software-Updates zeitnah durchführen, Schließen von Sicherheitslücken
- E-Mails genaustens checken und auf Phishing testen (PayPal, Handy...)
- Chat GPT nicht mit (sensiblen) Infos zum Unternehmen füttern
- Passwort-Manager mit konkreter Zugriffsberechtigung nutzen
- Cyberversicherung abschließen (Bedingungen + Kosten allerdings enorm)
- Sich bewusst werden, dass es Deepfake Videos, KI generierte Inhalte etc. gibt
- Website und CMS regelmäßig auf Sicherheit prüfen und aktuell halten
- Backup aller relevanten Daten, auf einem zweiten Server o.ä. anlegen

Auf Nachrichten vom C–Level zu Accountdaten, Zugängen o.ä. nicht einfach reagieren! Besser nochmal anrufen, nachfragen, ob die E-Mail wirklich von der entsprechenden Person kommt.

FAZIT

Fazit

Das Thema Cyberkriminalität und Hacking wird **zunehmend relevanter**: vor allem größere Unternehmen, die eine Menge an **relevanten Daten verarbeiten** sind für sogenannte Ransomware-Angriffe besonders interessant.

Es ist extrem wichtig, **nicht zu viel über sich preis zu geben** (insbesondere auch durch die neue Herausforderung ChatGPT). Sich als **Unternehmen ausreichend zu schützen**, ist heutzutage unabdingbar.

Mitarbeiter:innen sollten **regelmäßig geschult werden** und es sollte eine Person geben, die überprüft, dass **Passwörter regelmäßig geändert** werden.

Die Hacker informieren sich auch über die **Wirtschaftlichkeit eines Unternehmens**. Dort wo mehr zu holen ist, lohnt sich auch ein Angriff mehr.

Eine **doppelte Sicherung aller Daten und Informationen** sollte ebenfalls dringend in Erwägung gezogen werden.

Wenn es doch passiert ist: Für den Fall eines Hackerangriffs sollte ein **IT-Notfall-Plan** erarbeitet werden.

Text/Grafik:
© Klickkomplizen GmbH

Stand:
November 2023

Klickkomplizen

ONLINE MARKETING, WEB- UND PRINTDESIGN

/KLICKKOMPLIZEN