Hacker nutzen fortschrittlichste Werkzeuge

IT-Sicherheit: Geschäftsgeheimnisse, Daten und Online-Konten durch Multi-Faktor-Authentifizierung schützen

Passwörter sind eines der ältesten Sicherheitstools in der Welt der Softwareanwendungen und des Internets. Aber bieten sie unseren Unternehmen im IHK-Bezirk Coburg ausreichend Schutz? „Die IHK-Mitgliedsunternehmen müssen der Cyberkriminalität aktiv begegnen, denn für ihre Angriffe nutzen Hacker inzwischen künstliche Intelligenz, maschinelles Lernen, Phishing-Angriffe und Passwort-Leaks", appelliert IHK-Referent Rico Seyd.

Angriffe auf Unternehmen wie den Lebensmitteleinzelhändler Tegut (Fulda) und die FRÄNKISCHE Rohrwerke Gebr. Kirchner GmbH & Co. KG in Königsberg (Haßberge) zeigen, dass jedes Unternehmen Opfer eines Angriffs werden kann, unabhängig von Unternehmensgröße und Branche.

Die alleinige Authentifizierung durch Passwörter birgt folgende Risiken:

1. **Mitarbeiter verwenden dieselben Passwörter für unterschiedliche Anwendungen**
   Wenn ein Hacker Zugriff auf die Zugangsdaten eines Mitarbeiters z. B. für eine Anwendung erhält, besteht eine gute Chance, dass der Cyberkriminelle mit demselben Passwort in eine Unternehmensanwendung eindringen kann.
2. **Mitarbeiter verwenden leicht zu hackende Passwörter**
   Zusätzlich zur Wiederverwendung von Passwörtern neigen Menschen dazu, einfache und somit leicht zu hackende Passwörter zu wählen.
3. **Mitarbeiter bewahren ihre Passwörter nicht sicher auf**
   Selbst wenn sichere Passwörter verwendet werden, werden diese oft an unsicheren Orten hinterlegt. Angesichts der Schwierigkeit, sich Passwörter zu merken, ist es nicht verwunderlich, dass Mitarbeiter Passwörter in Word- oder Excel-Dokumente eingeben oder sogar auf Klebezettel schreiben.
4. **Schwache oder gestohlene Passwörter sind der wichtigste Einstiegspunkt für Hacker**
   Passwörter sind ein Top-Ziel für Hacker und stellen eine der am häufigsten vorkommenden Sicherheitsverletzungen dar.
5. **Auch privilegierte Konten sind häufig nicht besser geschützt**
   Erschwerend kommt hinzu, dass einige der privilegierten Konten möglicherweise unsichere Passwörter haben. Privilegierte Konten sind solche, die Zugriff auf vertrauliche Daten oder die Möglichkeit haben, Zugriff auf andere Anwendungen und Systeme zu gewähren. Beispiel: Administratorkonten.

Fortsetzung auf S. 22

Fortsetzung von S. 21

„Mehr Sicherheit schafft die Multi-Faktor-Authentifizierung kurz MFA. Bei der MFA handelt es sich um ein Verfahren, welches zwei oder mehr Faktoren bei der Authentifizierung kombiniert. Die verwendeten Faktoren können auf biometrischen Merkmalen (z. B. Fingerabdruck), speziellem Wissen (z. B. Antwort auf spezifische Frage) oder einem mitgeführten Gegenstand (z. B. Sicherheitstoken) basieren und sind voneinander unabhängig", erklärt Markus Vollmuth, Informationssicherheitsberater bei der atarax Unternehmensgruppe.

©terovesalainen - stock.adobe.com

Bei der sogenannten Multifaktor-Authentifizierung werden mehrere Sicherheitsverfahren gekoppelt.

Unternehmen, die MFA nutzen möchten, sollten die nachfolgenden Fragen für sich beantworten:

- Was soll durch die MFA geschützt werden?
- Welche Technologie soll eingesetzt werden?
- Wie „überzeugen" wir die Nutzer von dem neuen Authentifizierungsverfahren?

Es hat sich bewährt, die Einführung der MFA mit einer Art Informations- und Schulungskampagne zu begleiten, um zu verdeutlichen, dass MFA dazu da ist, die Mitarbeiter zu unterstützen und ihre Benutzerzugänge, Konten und alle ihre Daten zu schützen.

Soll MFA im gesamten Unternehmen ausgerollt werden, empfiehlt es sich, die privilegierten Konten, also die Admin-Konten, durch einen weiteren Faktor besser abzusichern.

Dieses Vorgehen hat zahlreiche Vorteile:

- Durch Absicherung der privilegierten Nutzerkonten schirmen Sie besonders wertvolle Ziele vor Hackern besser ab.
- Mittels „Inventarisation" der Nutzerkonten mit privilegierten Rechten, finden Sie heraus, welcher Nutzer administrative Rechte hat. So können Sie parallel überprüfen, ob diese Rechte wirklich notwendig sind und sie im Bedarfsfall einschränken.
- Zudem können Sie dieses Vorgehen als „Proof of Concept" nutzen, um das Erlernte für einen breiteren Einsatz zu nutzen.

Über die Nutzung von MFA empfiehlt es sich auch, bei der Einführung bzw. Umstellung auf Microsoft 365, aktuell Thema bei vielen Unternehmen, nachzudenken. Auch hier kann MFA die Sicherheit der Microsoft 365-Konten verbessern. Ein mehrstufiger Identitätsnachweis bei der Anmeldung verhindert schwerwiegende Datendiebstähle, weil Cyberkriminellen der unbefugte Zugriff auf die Cloud Dienste und Unternehmensdaten erschwert wird. ■

Autoren:
Rico Seyd, IHK zu Coburg, und Markus Vollmuth, atarax Unternehmensgruppe