Warnung: Microsoft-365-Konten leichte Beute!

23.07.2024, 22:53 | IT, New Media & Software

Pressemitteilung von: *ignition teams Waldkirch*

Mit uns zünden Organisationen

Erhöhtes Risiko für Unternehmen durch unzureichend geschützte M365-Konten. Der kürzlich erfolgte öffentlich bekannte Cyberangriff im Landkreis unterstreicht die Notwendigkeit einer robusten Sicherheitsinfrastruktur. Der Microsoft 365 Spezialist aus Waldkirch warnt alle Unternehmen und Organisationen, die M365 in irgendeiner Form einsetzen, vor möglichen Gefahren.

Ein nicht ausreichend gesichertes Konto kann als Einfallstor für Phishing-Angriffe, Ransomware und weitere schädliche Aktivitäten dienen, die nicht nur das betroffene Unternehmen, sondern auch dessen Kunden und Partner gefährden können. Die Folgen für Unternehmen oft gravierend. Diese können einen Datenverlust, einem finanziellen Schaden und vor allem die Schädigung der Reputation verursachen. Es ist einfach unangenehm, wenn der Chef allen Personen aus seinem Adressbuch, eine Nachricht schicken muss, und darin vor seinen eigenen Mails warnen.

Corona hat den Weg geebnet für Homeoffice und Mobile Work – ein attraktiver Arbeitsplatz ist nicht mehr der typische Tisch in einem Büro. Vorher war das eher die Ausnahme. Um die Kommunikation mit dem Büro und den Kunden ermöglichen wurde – oft zusätzlich der sonstigen IT-Infrastruktur – Microsoft Teams eingeführt. Ohne zu bemerken, dass die Einführung die Einrichtung eines M365-Kontos bedeutet hat. Sehr oft mit nur unzureichend sicherem Passwort. "War nur schnell für Videokonferenzen" hören die Fachleute oft in Kundengesprächen. Ein kleines Detail, ein Nebenschauplatz der aber eine große Wirkung nach sich ziehen kann.

Wie läuft so eine feindliche Übernahme ab? Der Chef eines Unternehmens bekommt von einem gut bekannten Geschäftspartner eine E-Mail mit einer Datenfreigabe, z.B. Dropbox oder ein Dokument zur Prüfung über Adobe Sign. Wer nicht genau hinschaut, ein gesundes Misstrauen hat, oder einfach im Stress ist, klickt auf den Link. Dann werden in einem Fenster die Zugangsdaten zu M365 abgefragt. Benutzername, Passwort und auch der Zweite Faktor. Genau betrachtet, sieht man diesen Seiten an, dass sie nicht echt sind. Oft übersehen dies die ungeschulten Laien. Werden die Zugangsdaten hier eingegeben sind diese gefished worden und werden in der Sekunde ausgenutzt. Das Adressbuch wird ausgelesen und weitere Mails an Geschäftspartner verschickt. Fällt dieser Hack nicht gleich auf, werden auch noch die Datenspeicher nach brauchbaren Inhalten durchsucht.

Wie schnell so ein Diebstahl von Zugangsdaten passieren kann, zeigt ignition teams in einem frei zugänglichen Video auf der Seite www.m365einfuehrung.de. Hier kann man sehen, wie gut diese auf das Opfer angepasste Phishing-Mail gemacht ist (Phishing ist Hacker-Jargon und beschreibt das Fischen nach Passwörtern) und wie glaubwürdig diese Mails wirken können. In dem vorgestellten Fall wurde ein SAP-Server von einem Kunden gehackt und alle gespeicherten Mail-

Adressen bekamen persönliche E-Mails von dem Geschäftsführer mit dem Ziel die Daten zu stehlen, für weitere Kontakte und die Möglichkeit vertraute Mails zu versenden. Diese Mail kam nur durch alle Sicherheitsmaßnahmen, da sie ja von einem bekannten Postfach einer bekannten Person kam. Das ist das perfide an dieser Vorgehensweise: die mit Geld bezahlbaren Sicherheitsmechanismen wie Spam- und Virenfilter sind hier oft nutzlos.

Ignition teams empfiehlt daher dringend, die Sicherheitsmaßnahmen zu überprüfen und zu verstärken. Hierbei sind die ausnahmslose Aktivierung der Multi-Faktor-Authentifizierung, die Nutzung von Sicherheits-Cloud-Diensten, die für die geschäftliche Nutzung konzipiert sind, sowie die Implementierung einer Datensicherung, die eine Wiederherstellung der Daten auch ohne Zugriff auf den Cloud-Account ermöglicht, nur die grundlegenden Maßnahmen, über die es normalerweise keine Diskussion geben sollte.

Die Sicherung eine Umgebung geht weit über den Einsatz eines der gängigen Schutztools hinaus: es gilt, die individuellen Zugriffsszenarien zu analysieren und zu sichern, Benutzer zu informieren und zu schulen. Kurz: es gibt keine Pauschallösung die einfach alles sicher macht.

Es ist von größter Bedeutung, dass Unternehmen die Risiken ernst nehmen und proaktiv handeln, um ihre und die Daten ihrer Kunden zu schützen. Ganz besonders Geschäftsführer und Inhaber sollten auf der Hut sein. Das oft zitierte "Was ist bei mir zu holen" ist ein gefährlicher Trugschluss. Erfolgreiche Manager haben viele interessante Kontakte im Postfach, die gilt es zu schützen.

Fachleute stehen bereit, um Unternehmen bei der Umsetzung effektiver Sicherheitsstrategien zu unterstützen und die digitale Sicherheit zu stärken. Ignition teams stellt allen Unternehmen eine Checkliste und Handlungsempfehlungen in einem umfassenden Dokument auf Anfrage zur Verfügung.

ignition teams GmbH

Fabrik Sonntag 4a
79183 Waldkirch
Deutschland

TimHaas (Gründer)

+49(7681)2064412

tim.haas@ignition-teams.de

www.m365einfuehrung.de/

Portrait

Die ignition teams GmbH entwickelt und implementiert zündende digitale Lösungen, mit denen Unternehmen aller Größenordnungen ihre Produktivität durch digitale Prozesse maximieren. Dabei liegt der Fokus auf einer umfassenden Bedarfsanalyse und Beratung, um passgenaue Konzepte zu entwickeln und betroffene Mitarbeiter frühzeitig zu involvieren. Auf Basis bewährter Methoden und vorhandener IT-Systeme setzt ignition teams anschließend automatisierte Abläufe im Unternehmen um, die langfristig für signifikante Wettbewerbsvorteile sorgen.

Durch das langjährige Arbeiten mit Cloud-Diensten haben sich die technischen Berater des Unternehmens eine Expertise im Sichern von Unternehmensdaten z.B. in Microsoft 365 erarbeitet. Viele Kunden und deren IT-Dienstleister sind in diesem relativ neuen Feld noch nicht so weit.

News-ID: 1265374 • Views: 480 (Stand: 03.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1265374/Warnung-Microsoft-365-Konten-leichte-Beute.html