beazley

Einblicke in die Branche

Bedrohung durch gestohlene Zugangsdaten: was Unternehmen wissen sollten

Jeden Tag kommt es bei Unternehmen und Websites zu Vorfällen im Bereich der Cybersicherheit, von denen einige zum Verlust von Kundendaten führen. Zu den kompromittierten Daten gehören häufig Listen von Benutzernamen und Passwörtern, mit denen die Angreifer auf Online-Ressourcen wie Websites und mobile Anwendungen zugreifen können. Diese Passwörter werden anschließend im Internet gehandelt und verkauft, zumeist auf Marktplätzen im Darknet, aber auch auf öffentlich zugänglichen Websites. Für gerade einmal 5 EUR ist es bereits möglich, an Passwortlisten heranzukommen. Zudem können Passwörter heutzutage problemlos falsch weitergegeben oder erraten werden, vor allem, wenn Benutzer immer noch schwache Passwörter verwenden (z. B. „Passwort“ oder „123456“). Hinzu kommt, dass eine Fülle von persönlichen Informationen online verfügbar ist, wodurch das Erraten noch einfacher wird.

Mit Passwörtern lässt sich viel Geld verdienen: Verschiedenen Studien zufolge besitzt eine durchschnittliche Person mehr als 150 verschiedene Konten im Internet. Viele Menschen machen sich aber nicht allzu viele Gedanken um ihre Passwortsicherheit und verwenden dasselbe Passwort für mehrere Konten. Mitunter nutzen sie sogar ein und dasselbe Passwort für persönliche Konten, vertrauliche Geschäftsanwendungen, auf die vom Internet aus zugegriffen werden kann, und für Remote-Verbindungen in das Unternehmensnetzwerk (über VPN oder Citrix). So kann ein kompromittiertes Passwort für ein persönliches Konto, selbst wenn es von einer Website stammt, auf der keine sensiblen Daten gespeichert sind, z. B. dailyquizz.me, den kriminellen Angreifern Zugang zu den Systemen eines Unternehmens verschaffen.

Für Angreifer ist es relativ einfach und auch kostengünstig, Credential-Stuffing-Angriffe durchzuführen. Hierbei handelt es sich um groß angelegte automatisierte Anmeldevorgänge mit gestohlenen Zugangsdaten (eine Authentifizierungsanfrage pro Benutzer). Das

Problem ist, dass diese Angriffe für IT-Sicherheitsteams oftmals nur schwer zu erkennen sind, da die Angreifer tatsächlich gültige Benutzernamen und Anmeldeinformationen verwenden, anstatt mittels „Brute-Force“ Zugangsdaten zu erraten.

Die Folgen eines solchen Angriffs hängen von der Art der Daten oder dem Zugang zu den kompromittierten Konten ab. Der Angreifer kann zum Beispiel Zugang zu einem Zeitschriftenabonnement erlangen, oder aber aus der Ferne mit speziellen Zugriffsrechten in die Informationssysteme eines Unternehmens eindringen. Es gibt jedoch mehrere Möglichkeiten, wie sich Ihr Unternehmen vor dieser Bedrohung schützen kann.

EINE DER WICHTIGSTEN MASSNAHMEN, DIE IHR UNTERNEHMEN ERGREIFEN KANN, IST DIE EINRICHTUNG DER MULTI-FAKTOR-AUTHENTIFIZIERUNG.

Das Konzept der Multifaktor-Authentifizierung (MFA) ist nicht neu. Vor der Erfindung von Schlüsseln (vor über 6.000 Jahren) mussten sich die Menschen durch eine geheime Nachricht ausweisen, um Zugang zu einem wichtigen Besprechungsraum zu erhalten. Viele Jahre später, als man herausfand, wie einfach es ist, eine geheime Nachricht zu erspähen oder zu erraten, wurden Schlüssel erfunden. Mit der Erfindung des Schlüssels kam die erste Version der Zwei-Faktor-Authentifizierung (2-FA) zum Einsatz: eine „Information“ (Standort der Tür) in Kombination mit einem „Objekt“ (physischer Schlüssel). Dasselbe Prinzip lässt sich heutzutage auch auf den sicheren IT-Zugang anwenden: Der Teil, den Sie „wissen“ (Benutzername und Passwort oder PIN), kann auch mehreren Angreifern bekannt sein. Hier kommt also der zweite Faktor, das „Objekt“, ins Spiel. Dabei kann es sich um ein Mobiltelefon oder eine SIM-Karte, einen Code, der auf einem physischen Token oder durch eine auf Ihrem Mobilgerät installierte Software generiert wird, oder ein vom Unternehmen registriertes Gerät handeln.

Die MFA erweist sich als eine sehr wirksame Methode, um Ihr Konto vor den oben genannten opportunistischen Angriffen zu schützen. Selbst wenn ein Angreifer Zugang zu einem gültigen Passwort erhält, würde der zweite Faktor Ihrer MFA verhindern, dass er sich damit in Ihren Online-Konten anmeldet.

Unlängst haben kriminelle Angreifer Tools entwickelt, um bestimmte MFA-Systeme zu umgehen. Manche dieser Tools wurden sogar veröffentlicht (z. B. EvilProxy).

Erst kürzlich gab es zwei größere Vorfälle, bei denen die MFA umgangen wurde:

- Der erste Angriff betraf Uber. Der Angreifer verschaffte sich zunächst Zugang zu den Systemen des Unternehmens, indem er das Konto eines einzelnen Mitarbeitenden (dessen Passwort zuvor kompromittiert worden war) ins Visier nahm und diesem wiederholt MFA-Push-Benachrichtigungen schickte. Nach gut einer Stunde kontaktierte der Angreifer denselben Mitarbeitenden über WhatsApp und gab sich als Mitglied des IT-Supports von Uber aus. Er teilte ihm mit, dass keine MFA-Benachrichtigungen mehr übermittelt würden, sobald die Zielperson die Anmeldung bestätigt hätte. Dies tat der

Mitarbeitende auch, wodurch der Angreifer sofort direkten Zugang erhielt.

- Der zweite Vorfall ereignete sich bei Twilio, wo Angestellte per SMS auf gefälschte Anmeldeseiten umgeleitet wurden. Dadurch konnte der Bedrohungsakteur die MFA-Tokens auslesen und sie verwenden, um sich aus der Ferne im System anzumelden (hier finden Sie ein Beispiel dafür, wie die MFA umgangen werden kann).
  Nicht alle MFA-Lösungen bieten das gleiche Maß an Sicherheit. In den meisten Fällen werden bei der Umgehung der MFA schwache Konfigurationspraktiken ausgenutzt, die durch eine Änderung der Standardkonfiguration behoben werden können (z. B. durch Blockieren der Legacy-Authentifizierung). Auf diese Weise können schwächere MFA-Lösungen mit der richtigen Sicherheitskonfiguration sicherer gestaltet werden (weitere Informationen erhalten Sie in den Empfehlungen von Microsoft).

Sicherheitsbewusstsein und sichere Passwörter sind ebenfalls unerlässlich

Das Sicherheitsbewusstsein ist nach wie vor ausschlaggebend dafür, dass einzelne Mitarbeitende sich beim Umgang mit Passwörtern richtig verhalten. Darunter fällt die Verwendung von eindeutigen, langen und/oder komplexen Passwörtern, die nicht anhand der Informationen, die im Internet zu finden sind, erraten werden können, z. B. der Vor- und Nachname eines Benutzers, der Firmenname oder die Adresse. Ein persönlicher Passwort-Manager (z. B. Bitwarden, der kostenlos und quelloffen ist), kann eine gute Lösung sein, um eindeutige und komplexe Passwörter für jedes einzelne Online-Konto einfach und schnell zu erzeugen und zu speichern. Außerdem ist es wichtig, Mitarbeitende in der Erkennung von gefälschten oder manipulierten Domainnamen zu schulen, um sich gegen die neuesten Methoden zur Umgehung der MFA zu schützen.

Wenn Unternehmen von ihren Mitarbeitenden oder Kunden nicht erwarten, dass sie sich von einem bestimmten Ort aus mit den Systemen des Unternehmens verbinden, können sie Fernverbindungen aus anderen Ländern, Regionen oder Kontinenten kontrollieren, indem sie geografische Standortbeschränkungen einführen. Je nach Standort und Zeitpunkt des Verbindungsversuchs kann ein Unternehmen entscheiden, ob es einen Verbindungsversuch blockiert oder zusätzliche Nachweise über einen dritten Faktor wie einen per E-Mail gesendeten Link, eine Frage mit einer vorkonfigurierten geheimen Antwort, einen Telefonanruf oder eine Benachrichtigung auf einem mobilen Gerät verlangt.

Eine weitere Möglichkeit für Unternehmen, die Sicherheit von Passwörtern zu erhöhen, ist die Überwachung von veröffentlichten Anmeldedaten. Manche Unternehmen, die von einem Datenleck betroffen sind, machen sich die Mühe, die von dem Vorfall betroffenen Kunden und Mitarbeitenden zu benachrichtigen, andere jedoch nicht. Es kann jedoch hilfreich sein, zu wissen, wann Daten und Passwörter gestohlen wurden, um bei Bedarf entsprechende Maßnahmen zu ergreifen. Z. B. sollten Passwörter, die für mehrere Konten verwendet werden, geändert werden, eine nicht aktivierte MFA sollte aktiviert werden oder die Bank sollte informiert werden, wenn Kreditkarteninformationen gestohlen wurden. Es gibt mehrere

Websites, über die Interessierte erfahren können, ob ihre Daten bei öffentlich bekannt gewordenen Sicherheitsverletzungen offengelegt wurden (wie haveibeenpwned.com).

Passwort-Manager (darunter auch Bitwarden und der Passwort-Manager von Google Chrome) verfügen über Funktionen, mit denen Benutzer herausfinden können, ob ihre Passwörter in bekannt gewordenen Datenlecks offengelegt wurden. Diese Funktionen werden oft kostenlos angeboten. Es gibt außerdem spezialisierte Dienstleister, die Unternehmen benachrichtigen, wenn ihre Daten im Darknet gefunden werden, teils sogar noch bevor die Sicherheitslücke öffentlich bekannt wird. Diese Dienstleistung wird oft als „Dark Web Monitoring“ bezeichnet.

Da kriminelle Angreifer auch in Zukunft versuchen werden, leichte Opfer zu finden, sind Sicherheitsverfahren wie die Einführung einer sicheren MFA und Richtlinien für sichere Passwörter unverzichtbare Bestandteile des Risikomanagements eines jeden Unternehmens. Es lohnt sich also, sich selbst und Kolleginnen und Kollegen über die neuesten Risiken zu informieren und Maßnahmen zur Risikominderung zu ergreifen.

beazley