carmasec

security. done. right.

Identitätsdiebstahl

Gestohlene Zugangsdaten im Unternehmenskontext

Whitepaper 10/2021

carmasec

Über das Whitepaper

Während unterschiedlichste IT-Sicherheitsmaßnahmen bei Unternehmen bekannt sind, wird die Bedrohung durch eine Kompromittierung der Passwörter von Mitarbeiter:innen oft unterschätzt. In der Regel fällt der Diebstahl unternehmenseigener Zugangsdaten erst auf, wenn bereits große Schäden angerichtet wurden. Um sich hiervor effektiv zu schützen, benötigen Unternehmen eine systematische Herangehensweise zur Auswahl und dem Einsatz geeigneter Maßnahmen.

In diesem Whitepaper werden typische Angriffsvektoren des Identitätsdiebstahls erläutert. Dazu gehören beispielsweise die Mehrfachnutzung von Passwörtern sowohl im unternehmerischen als auch im privaten Kontext sowie die Verwendung von schwachen Zugangsdaten, die für Kriminelle leicht zu erraten sind. Zudem werden sieben Security-Tipps vorgestellt, mit denen Unternehmen die eigene Sicherheit bezüglich der Passwort-Authentifikation deutlich ausbauen können.

Inhalt

ZUM AUTOR

Dr. Timo Malderle ist Cyber Security Consultant bei der auf Cybersicherheit spezialisierten Beratungsboutique carmasec GmbH & Co. KG mit Hauptsitz in Essen.

Bei seinen Kunden bringt Timo Malderle u.a. sein Expertenwissen für Identity- and Access Management ein. Als Experte für IT-Security beschäftigte er sich während seiner Promotion mit der Warnung von Betroffenen, deren Passwörter und Identitäten gestohlen wurden.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Kompromittierte Passwörter – ein unterschätztes Risiko

Unternehmensabläufe werden zunehmend digitalisiert und durch IT-Prozesse unterstützt. Wichtige interne Vorgänge werden dadurch systemgestützt realisiert und auch Unternehmensgeheimnisse werden digital verwaltet. Aufgrund des erheblichen Wertes dieser Vorgänge und Daten haben Kriminelle ein stetig wachsendes Interesse, illegal Zugriff darauf zu bekommen. Sie finden immer wieder neue und kreative Wege, um an solche Daten zu gelangen. Viele IT-Verantwortliche sind sich der Bedrohungen durch Malware und Phishing bewusst und investieren deshalb in Maßnahmen der Malware-Protection und in Anti-Phishing-Trainings. Dagegen wird der Angriffsvektor rund um kompromittierte Passwörter in einem Großteil der Unternehmen übersehen.

Diesen Blind-Spot nutzen Cyberkriminelle seit einigen Jahren immer effektiver aus, um einen Zugang in die anzugreifende Unternehmens-Infrastruktur zu erhalten. Viele Cyberangriffe verwenden als Einstiegsvektor kompromittierte Log-in-Daten von Mitarbeitenden, um auf dem Weg die Zugriffsrechte der jeweiligen Person auszunutzen. Diese Art von Identitätsdiebstahl führt bei den betroffenen Unternehmen zu immensen Schäden, die existenzbedrohend sein können. Aus diesem Grund ist es *carmasec* wichtig, ein Bewusstsein für das Risiko des Identitätsdiebstahls bei Unternehmen zu erzeugen und geeignete Ansätze zur Mitigation aufzuzeigen.

Angriffsvektoren auf die Zugangsdaten von Mitarbeiter:innen

Das klassische Passwort ist nach wie vor die sowohl im privaten Umfeld als auch in Unternehmen vorherrschende Methode zur Benutzer-Authentifizierung. Die notwendigen Ressourcen für die Implementierung und den Betrieb auf der Systemseite sind im Vergleich zu anderen Verfahren vollständig zu vernachlässigen. Auch auf der Seite der Benutzer:innen ist das Verfahren von Passwörtern etabliert. Es bedarf hierfür keines gesonderten Schulungsaufwandes. Jedoch sind viele Personen mit ihrem Passwortmanagement überfordert. Die Menge an beruflich und privat genutzten Diensten führt zu einer unübersichtlichen Anzahl von Passwörtern. Müssen diese dann noch alle drei Monate geändert werden, resignieren viele Benutzer:innen. Als Folge werden unsichere und leicht zu merkende Passwörter verwendet oder es kommt nur „ein Passwort für alles“ zum Einsatz.

Um zu verstehen, wie Identitätsdaten abhanden kommen können, wird zunächst die Authentifikation mit Passwörtern genauer betrachtet. Als Grundsatz wird bei der Passwort-Authentifikation zwischen Benutzer:in und Dienst ein Geheimnis vereinbart. Der Benutzer beweist dem Dienst seine Identität, indem er das geteilte Geheimnis nennt. Diese Art der Authentifikation bedingt, dass das vereinbarte Geheimnis – in Form des Passworts – auch geheim gehalten wird.

ⓘ Identitätsdiebstahl vs. Identitätsdatendiebstahl

Werden Zugangsdaten wie E-Mail-Adresse und Passwort gestohlen, ohne diese für eine Anmeldung bei dem zugehörigen Dienst zu verwenden, wird von einem *Identitätsdatendiebstahl* gesprochen. Werden diese Daten für einen Betrug eingesetzt, ist dies ein *Identitätsdiebstahl*. [1]

Erfährt eine dritte Instanz von diesem Geheimnis, dann muss dieses Benutzerkonto zwingend als kompromittiert angesehen werden, weil sich nicht nur die Person, sondern auch die dritte Instanz als legitimer User ausgeben kann.

Diese dritte Instanz kann auf verschiedenen Wegen Kenntnis von dem eingesetzten Passwort erlangen:

Data-Breaches

Kriminelle nutzen Fehlkonfigurationen oder Sicherheitslücken in den von Unternehmen eingesetzten Systemen aus, um Zugriff auf die Infrastruktur zu erhalten. Gelegentlich gelingt es ihnen sogar, die vollständige Benutzerdatenbank zu kopieren und zu entwenden. Die gestohlenen Zugangsdaten werden dann im großen Stil in bestimmten Bereichen des Internets gehandelt und verbreitet. Auch bekannte Onlinedienste werden immer wieder Opfer solcher Angriffe. Als Folge kursieren Benutzerdatensätze mit E-Mail-Adressen und Passwörtern im Internet, die eine Datenmenge von mehreren Gigabyte deutlich überschreiten können.

Passwort-Wiederverwendung

Personen empfinden das Ausdenken, Merken und Eingeben von Passwörtern in der Regel als besonders lästig, da sie meist mehr als nur ein Benutzerkonto haben. Je sicherer ein Passwort sein soll, desto aufwendiger wird der Prozess des persönlichen Passwortmanagements. Untersuchungen haben ergeben, dass eine Person im Durchschnitt zwischen 25 und 207 Benutzerkonten besitzt [1]. Jedoch ist schon das Merken von 25 sicheren Passwörtern eine Herausforderung. Deshalb verwenden mehr als die Hälfte aller Benutzer:innen ihre Passwörter mehrfach [2,3,4].

Eine durchschnittliche Person verwendet 79 % der eigenen Passwörter mehrfach [2]. Starke Passwörter und Passwörter, die oft eingegeben werden müssen, werden häufiger mehrfach verwendet [5].

Der Grundsatz der Passwort-Authentifikation fordert, dass ein Passwort nur zwischen Benutzer:in und Dienst (Dienst A) geteilt werden darf. Verwendet eine Person das gleiche Passwort auch bei einem anderen Dienst (Dienst B), dann verrät sie einer dritten Instanz das vereinbarte Geheimnis. Ab diesem Zeitpunkt ist das Passwort kompromittiert, weil das Schutzziel der Vertraulichkeit nicht mehr gewährleistet werden kann. Technisch bekommt der zweite Dienst (Dienst B) das Passwort im Klartext übermittelt und ist somit in der Lage, sich bei dem ersten Dienst (Dienst A) anzumelden. Die Person muss Dienst B zu 100 % vertrauen, dass dieser mit dem Passwort verantwortungsvoll umgeht. Eine technische Sicherung, dass Dienst B das Passwort nicht missbraucht, ist bei der Mehrfachverwendung eines Passwortes nicht mehr gegeben. Auch wenn Dienst B eine hohe Vertrauenswürdigkeit besitzt, kann es Angreifenden gelingen, bei Dienst B die Zugangsdaten der Person zu entwenden. Spätestens dann muss damit gerechnet werden, dass die entwendeten Zugangsdaten auch bei Dienst A ausprobiert werden.

Für ein Unternehmen bedeutet die mehrfache Verwendung von Passwörtern, dass ein Sicherheitsvorfall bei einem fremden Dienst zu einer akuten Bedrohung der eigenen Infrastruktur führt. Bei einem solchen Vorfall spielt es keine Rolle, wie sicher die Infrastruktur eines Unternehmens und wie komplex das kompromittierte Passwort ist. Wenn Dienst B seine Infrastruktur nicht sichert, dann ist auch Dienst A betroffen.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Unsachgemäßer Umgang durch den Benutzenden

Das notwendige Bewusstsein für den richtigen Umgang mit Passwörtern fehlt oftmals bei Benutzer:innen. Sie neigen dazu, die Sicherheit aus Bequemlichkeit zu vernachlässigen. Beispielsweise werden Zugangsdaten mit Teammitgliedern geteilt, damit diese während der Urlaubsvertretung auf die entsprechenden Systeme zugreifen können, anstatt die notwendigen Berechtigungen bei der IT zu beantragen. Auch werden Passwörter auf Notizzetteln an den Computerbildschirm geheftet.

Viel weitreichender wird das Problem, wenn Benutzer:innen die Unternehmenszugangsdaten bewusst mit anderen Diensten teilen. Für diese Personen sehr verlockend sind hier beispielsweise sogenannte Workflow-Automation-Services. Diese Dienste ermöglichen es, Funktionen mehrerer Onlinedienste miteinander zu verknüpfen. So lassen sich beispielsweise Einträge aus einer externen ToDo-Listen-Applikation direkt als Termin in den Unternehmenskalender übertragen. Damit diese Automatisierung möglich wird, muss der Workflow-Automation-Service Zugriff auf die Benutzerkonten bei den entsprechenden Diensten besitzen. Manche Dienste lösen diese Funktion technisch sauber mit einem Berechtigungsmanagement und Single-Sign-On. Jedoch sind auch Lösungen auf dem Markt, bei denen Benutzer:innen die eigenen Zugangsdaten im Klartext für die zu verknüpfenden Dienste hinterlegen muss. Wenn hier beispielsweise das Exchange-Konto eines Teammitglieds eingebunden wird, hat der genutzte Workflow-Automation-Service Vollzugriff auf das E-Mail-Postfach der Person. Auch hier kann es sich natürlich um einen vertrauenswürdigen Dienst handeln, der verantwortungsvoll mit den Zugangsdaten umgeht.

Ein Sicherheitsvorfall bei einem solchen Workflow-Automation-Service kann jedoch dazu führen, dass das eigene Unternehmen ebenfalls Opfer von Cyber-Angriffen wird.

Verwendung schwacher Passwörter

Benutzer:innen tendieren dazu, kurze und gebräuchliche Passwörter zu verwenden. Das durchschnittliche Passwort hat eine Länge von acht bis neun Zeichen. Häufig werden einfache Wörter oder sehr simple Konstruktionen für die Erstellung eines Passwortes verwendet. Dies führt dazu, dass ein Passwort nicht selten bereits von tausenden Personen benutzt wird.

Als Sicherheitsmaßnahme zwingen viele Unternehmen ihre Mitarbeitenden dazu, alle drei Monate ein neues Passwort zu vergeben. Obwohl diese Lösung schon seit vielen Jahren umstritten und seit einigen Jahren vom BSI und der NIST auch als kontraproduktiv eingeschätzt wird, ist sie dennoch in vielen Betrieben im Einsatz. Diese Maßnahme ist aber aus mehreren Gründen kritisch für die Sicherheit des Unternehmens. Wird das Benutzerkonto eines Mitarbeitenden kompromittiert, dann reichen einem Angreifer häufig schon wenige Minuten, um zumindest einen ersten Schaden anzurichten. Wenn dann nach drei Monaten das Passwort des bereits missbrauchten Benutzerkontos geändert wird, trägt das nicht wirklich zur Schadensminimierung bei, weil in diesem Zeitraum schon sämtliche Unternehmensgeheimnisse entwendet und die gesamte digitale Infrastruktur zerstört worden sein kann. Kritisch ist zudem, dass die gewählten Passwörter durch einen erzwungen Passwortwechsel meist deutlich unsicherer sind. Anstatt sich einmal ein wirklich sicheres Passwort zu überlegen, tendieren Menschen bei einem erzwungenen Passwortwechsel dazu, ein Passwort zu wählen, das möglichst einfach zu merken ist.

Angreifer entwickeln immer neue Ideen, um die Risiken von schwachen Passwörtern auszunutzen. Beispielsweise wählen sie einen bestimmten Benutzernamen aus und probieren dann, sich mit häufig genutzten Passwörtern anzumelden - dies natürlich voll automatisiert. Auf diese Art und Weise gelingt es ihnen immer wieder, Zugriff auf die entsprechenden Benutzerkonten zu erlangen. Grund für den Erfolg sind auch die eingesetzten Methoden. Es werden genau für diese Angriffe hochkomplexe Systeme entwickelt, die mit Verfahren der künstlichen Intelligenz wahrscheinliche Passwörter aus gesammelten Informationen ableiten. Die Erfolgsquoten dieser Methoden für Passwörter mit geringer Komplexität und Länge sind sehr hoch.

Weitere Angriffsvektoren

Verschiedene Arten an Malware können dazu genutzt werden, Zugangsdaten zu entwenden. Beispielsweise kann ein Keylogger die Passworteingaben einer Person aufzeichnen und zum Angreifer senden. Die Malware-Protection in Unternehmen ist deshalb eine essenzielle Sicherheitsmaßnahme.

Aber auch die Bedrohung durch Brute-Force-Angriffe sollten Unternehmen kennen. Bei Brute-Force-Angriffen probieren Kriminelle alle möglichen Passwörter solange aus, bis ein Anmeldeversuch mit dem richtigen Passwort geglückt ist. Dafür sind in der Regel sehr viele Versuche notwendig. Die Anzahl an möglichen Anmeldeversuchen innerhalb eines Zeitraums bestimmt die Erfolgsaussichten. Betreibt ein Unternehmen ein öffentliches Anmelde-Interface, bei dem mehrere tausend Anfragen von einer IP-Adresse pro Sekunde möglich sind, dann werden Cyberkriminelle diese Möglichkeit mit hohen Erfolgsaussichten ausnutzen.

Eine geeignete Gegenmaßnahme ist hier, dass alle Anmelde-Interfaces und APIs nur eine begrenzte Anzahl an Anfragen innerhalb eines Zeitraumes zulassen und Anfragen von IP-Adressen mit zu vielen Versuchen blockieren.

Bedrohung durch Identitätsdiebstahl

Sind die Zugangsdaten von Mitarbeitenden eines Unternehmens erst einmal abhanden gekommen, entstehen Bedrohungen unterschiedlichster Art und mit einem kaum überschaubaren Risiko. Untersuchungen zeigen, dass nicht selten kompromittierte Zugangsdaten im Internet für mehrere Jahre kursieren, die betroffene Person oder das Unternehmen hiervon aber nichts mitbekommt und die sich im Umlauf befindlichen Zugangsdaten immer noch verwendet werden.

Die kompromittierten Zugangsdaten können von Angreifenden als Sprungbrett genutzt werden, um über eine längere Zeit die Unternehmensinfrastruktur auszuspionieren und in weitere Systeme einzudringen. Beispielsweise durch Spionage oder gezielte Installation von Ransomware können sie so einen immensen Unternehmensschaden verursachen. Diese Art von Angriffen, auch Advanced-Persitent-Threats (APT) genannt, sind durch den langen Zeitraum und den geringen Automatisierungsgrad schwer zu erkennen und die entstehenden Schäden umso größer.

Die Ziele dieser Angriffe sind ähnlich komplex wie die Angriffe selbst. Häufige Intentionen sind die Unternehmensspionage, die Manipulation von Unternehmensgeheimnissen, die Erpressung im Rahmen eines Ransomware-Angriffs oder aber die bloße Zerstörung von Unternehmensinfrastruktur und Unternehmensinformationen aus rein ideologischen Gründen.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

7 Security-Tipps zur Risikominimierung

Nachdem die möglichen Angriffsvektoren und der daraus resultierende Schaden aufgezeigt wurden, werden nun sieben Security-Tipps zur Risikominimierung dieser Bedrohungen genannt. Mit den folgenden Maßnahmen können Personen und Unternehmen den zuvor genannten Gefahren entgegenwirken:

SECURITY-TIPP 1

Umsetzung von Standard-Sicherheitsmaßnahmen

Auch wenn dieser Tipp selbstverständlich klingt, ist die gelebte Realität in vielen Unternehmen eine andere. Es ist zwingend notwendig, die eingesetzte Software regelmäßig mit Updates zu versorgen, um so schnellstmöglich gefundene Sicherheitslücken in den Systemen zu schließen. Hierfür ist ein vollständiges Patch-Management notwendig, das sämtliche Serversysteme und Anwendungen mit einbezieht.

Auch Fehlkonfigurationen in der eingesetzten Software müssen vermieden werden. Allzu häufig werden Datenbanken betrieben, die aus dem Internet erreichbar sind und für die keine Benutzerauthentifizierung mit einem Passwort eingerichtet worden ist. Das heißt, dass diese Datenbanken unbeabsichtigt öffentlich zugänglich betrieben werden. Hier hilft es, die betriebenen Systeme und deren Konfiguration zu dokumentieren und generell Konzepte für den Betrieb solcher Systeme vorzuhalten. Darüber hinaus ist ein geeignetes Malware-Schutzkonzept notwendig, das sämtliche Systeme im Unternehmensnetz vor dem Befall mit Malware schützt.

SECURITY-TIPP 2

Kompromittierte Zugangsdaten erkennen und deaktivieren

Für Unternehmen ist es wichtig, die eigene Bedrohungslage konkret einschätzen zu können. Einen großen Einfluss auf die Unternehmenssicherheit haben Benutzerkonten, da Cyberkriminelle mit Hilfe eines kompromittierten Benutzerkontos unbemerkt Zugriff auf die Unternehmensinfrastruktur bekommen. Ein Angreifender, der sich mit validen Zugangsdaten anmeldet, ist nur schwer vom echten Benutzer zu unterscheiden. Ebenfalls ist es schwer zu detektieren, wann ein Angreifender gestohlene Zugangsdaten für welche Aktionen missbraucht. Aus diesem Grund ist es sinnvoll, dass Unternehmen regelmäßig überprüfen, ob Zugangsdaten von Benutzer:innen kompromittiert wurden. Hier bieten sich verschiedene Dienste an, die das Darknet nach gestohlenen Zugangsdaten durchsuchen und Unternehmen vor kompromittierten Zugangsdaten warnen. Aus einer Warnung bezüglich kompromittierter Zugangsdaten lassen sich zwei Hinweise auf Schwachstellen der Unternehmenssicherheit ableiten: Erstens haben Angreifende die Möglichkeit, sich unbemerkt als der entsprechende Benutzer auszugeben. Zweitens gibt es eine Schwachstelle, über die das entsprechende Passwort entwendet wurde. Aus diesem Grund sind bei kompromittierten Benutzerkonten mehrere Aktionen notwendig:

- kompromittierte Benutzerkonten unverzüglich deaktivieren
- untersuchen, ob forensische Hinweise existieren, dass Angreifer bereits die Zugangsdaten für eine Anmeldung im Unternehmensnetz missbraucht haben
- untersuchen, wie das Passwort abhanden kommen konnte

SECURITY-TIPP 3

Die eigene Passwort-Policy überprüfen

Wenn es eine Passwort-Policy in Unternehmen gibt, dann ist diese häufig nicht zielführend. In den meisten Passwort-Policies wird eine Angabe zur Mindestlänge und zu den enthaltenen Zeichenarten gemacht. Ebenfalls wird häufig der Hinweis gegeben, dass Passwörter nicht notiert werden dürfen und alle drei Monate geändert werden müssen.

Durch eine Änderung oder Ergänzung einzelner Aspekte kann aber ein spürbarer Sicherheitsgewinn herbeigeführt werden:

Die notwendige Passwortlänge wird häufig auf acht Zeichen festgelegt. Hierbei sollte hinterfragt werden, ob acht Zeichen tatsächlich ausreichend sind. Für eine solche Entscheidung muss der Schutzbedarf der einzelnen Benutzerkonten festgestellt werden.

Der regelmäßige Passwortwechsel-Zwang muss unbedingt deaktiviert werden, denn sowohl wissenschaftliche Forschung als auch BSI und NIST raten hiervon ab.

In einer Passwort-Policy muss festgehalten werden, dass ein Unternehmenspasswort nicht bei externen Diensten verwendet werden darf, besonders nicht im privaten Kontext.

Die Orte, an denen ein Passwort eingegeben werden darf, müssen limitiert werden. Dies wird durch das Unternehmen in der Passwort-Policy dokumentiert.

Den Mitarbeiter:innen muss untersagt sein, ein Unternehmenspasswort bei externen Diensten zu hinterlegen, um dadurch beispielsweise die zuvor genannten Workflow-Automation-Services zu nutzen.

SECURITY-TIPP 4

Umsetzung der Passwort-Policy

Es reicht nicht aus, notwendige Maßnahmen und Vorgaben nur in einer Policy zu dokumentieren. Diese muss auch im Unternehmen realisiert werden. Damit Mitarbeiter:innen mit den entsprechenden Regeln umgehen können, empfiehlt es sich, die in der Passwort-Policy dokumentierten Vorgaben in Security Awareness-Trainings zu schulen. Zudem ist es bei der Regelung des Passwortumgangs wichtig, auch die Usability mit einzubeziehen. Eine häufig formulierte Anforderung in Passwort-Richtlinien ist, dass Passwörter nicht notiert werden dürfen. Wenn ein Teammitglied jedoch viele unterschiedliche Systeme mit verschiedenen Benutzerkonten verwendet, bleibt ihm kaum etwas anderes übrig, als Passwörter aufzuschreiben oder wiederzuverwenden. Hierbei können Mitarbeiter:innen durch Passwortmanager unterstützt werden. Über diese können sichere und individuelle Passwörter genutzt werden, ohne die Anwendenden zu überfordern.

Darüber hinaus sollte überprüft werden, ob auch alle Systeme die geltende Passwort-Policy technisch umsetzen. Es ist kontraproduktiv, wenn in den Richtlinien eine Mindestlänge von zehn Zeichen bei der Wahl eines Passworts vorgegeben werden, vom System aber nur vier Stellen akzeptiert werden.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Ebenfalls kann die Qualität von Passwörtern verbessert werden, wenn schlechte oder bereits kompromittierte Passwörter nicht wiederverwendet werden. Hierfür ist die Überprüfung des Passworts auf Systemebene notwendig.

SECURITY-TIPP 5

Zwei-Faktor-Authentifizierung einführen

Die reine Passwort-Authentifizierung lässt sich zwar am einfachsten implementieren, bietet aber nicht den besten Schutz. Bei Onlinediensten und Banken ist die Verwendung eines zweiten Faktors bei der Anmeldung schon weit verbreitet. Die Einführung eines zweiten Faktors auch im Unternehmenskontext bringt einen signifikanten Sicherheitsgewinn. Gerade für Benutzerkonten mit vielen Systemrechten bietet sich die Verwendung an. Soll ein zweiter Faktor im Unternehmen eingeführt werden, müssen geeignete Produkte ausgewählt werden, die sich bestmöglich in die bestehende Infrastruktur integrieren lassen.

SECURITY-TIPP 6

Benutzer:innen durch Awareness-Schulungen sensibilisieren

Gerade im Bereich der Passwort-Authentifikation haben die Mitarbeitenden eines Unternehmens essenziellen Einfluss auf die Unternehmenssicherheit. In entsprechenden Awareness-Schulungen kann ihnen vermittelt werden, dass sie durch die Verwendung guter Passwörter zur Verbesserung der Sicherheit im Unternehmen beitragen können. Bei schon existierenden Awareness-Schulungen im Bereich der IT Security ist meistens das Thema Phishing sehr präsent, der richtige Umgang mit Passwörtern ist jedoch oftmals unterrepräsentiert oder gar nicht vorhanden.

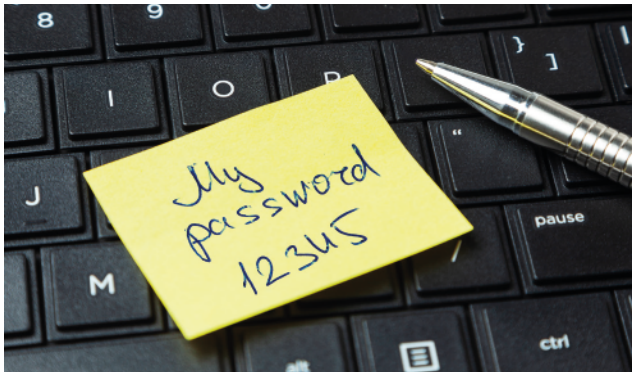
SECURITY-TIPP 7

Technische Schutzmaßnahmen implementieren

Soweit es möglich ist, Maßnahmen technisch abzusichern, sollte das auch realisiert werden. Sämtliche Login-Interfaces eines Unternehmens sollten ein Limit implementiert haben, das nur eine bestimmte Anzahl an gescheiterten Anmeldeversuchen akzeptiert. Hierfür müssen zunächst einmal alle Anmelde-Interfaces zusammengetragen werden: Login-Formulare auf Websites, APIs und zentrale Verzeichnisdienste mit den angebundenen Services.

Hierbei ist insbesondere auf die vom Internet aus zugänglichen Interfaces zu achten, da bei einer fehlenden Limitierung der Anmeldeversuche der Angreifende automatisiert Passwörter erraten kann. Sollte eine maximale Anzahl an gescheiterten Anmeldeversuchen durchgeführt worden sein, so ist es zielführend, die entsprechende IP-Adresse zu blockieren.

Eine weitere technisch realisierbare Maßnahme ist die Deaktivierung des Zugriffs aus dem Unternehmensnetz auf bekannte risikobehaftete Dienste. Stehen externe Onlinedienste mit einer internen Sicherheitsrichtlinie in Konflikt, ist es sinnvoll, den Zugriff auf diesen Dienst auch technisch zu sperren. Beispielsweise kann so verhindert werden, dass ein Mitarbeitender einen unerwünschten Workflow-Automation-Service einrichtet.



Fazit

Es wurde eine Reihe an Möglichkeiten vorgestellt, wie in Unternehmen die eigenen Zugangsdaten kompromittiert werden können. Die Gefahren sind vielseitig und erfordern Maßnahmen sowohl auf der Technik-Ebene als auch auf der Ebene der Mitarbeiter:innen. Die sieben Security-Tipps geben einen Überblick über notwendige und hilfreiche Maßnahmen. Bei der Realisierung dieser Tipps kann es für Unternehmen gerade bei den komplexeren Themen ratsam sein, externe Expertise einzuholen, damit die Maßnahmen korrekt und vollständig implementiert werden.

Literaturverzeichnis

[1] Malderle: ***Bedrohung durch Identitätsdatendiebstahl: Datenerhebung, Analyse und Mitigation***. - Bonn, 2021. - Dissertation, Rheinische Friedrich-Wilhelms-Universität Bonn.

[2] Pearman et al.: ***Let's Go in for a closer look: Observing passwords in their natural habitat***. In: Proceedings of the ACM Conference on Computer and Communications Security. New York, 2017.

[3] Wang et al.: ***The next domino to fall: Empirical analysis of user passwords across online services***. In: CODASPY 2018 - Proceedings of the 8th ACM Conference on Data and Application Security and Privacy. New York, 2018.

[4] Web.de: ***Was ist Ihre bevorzugte Methode, die notwendige Menge an Passwörtern zu verwalten?*** 2019. https://www.slideshare.net/WEBDE_DEUTSCHLAND/passwortstudie-59-der-deutschen-internetnutzer-verwenden-passwrter-mehrfach

[5] Wash et al.: ***Understanding Password Choices: How Frequently Entered Passwords Are Reused across Websites***. Denver, 2016. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

SO UNTERSTÜTZEN WIR BEI DER SICHERUNG VON IDENTITÄTS- UND ZUGANGSDATEN

1. Schritt: Bestandsaufnahme

Gemeinsam analysieren wir Ihre aktuellen Maßnahmen zum Schutz von Zugangsdaten und identifizieren potentielle Schwachstellen.

2. Schritt: Maßnahmen planen und umsetzen

Auf Basis unserer Ergebnisse aus der Analyse definieren wir individuell für Ihr Unternehmen pragmatische Maßnahmen und planen deren Umsetzung.

3. Schritt: Beobachten und Optimieren

Wir prüfen regelmäßig die Effektivität, Angemessenheit und Compliance der umgesetzten Maßnahmen und passen diese im Bedarfsfall an.

SIE HABEN FRAGEN? SPRECHEN SIE MICH AN.

Jan Sudmeyer
Managing Partner &
Senior Trusted Advisor

UNSERE KONTAKTDATEN

www.carmasec.com
contact@carmasec.com
+49 (0) 201 426 385 900
xing.carmasec.com
twitter.carmasec.com
linkedin.carmasec.com

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

carmasec
security. done. right.

ÜBER CARMASEC

carmasec ist eine im Jahr 2018 in Deutschland gegründete Beratungsboutique für Cybersicherheit. Als „Trusted Advisor“ im Bereich der Cyber-Resilienz bieten wir unseren nationalen und internationalen Kunden professionelle Beratungsleistungen und Lösungen. Unsere Expertise liegt in den Themenfeldern Cloud Security, Informationssicherheit, DevSecOps, Identity & Access Management, Risikomanagement, Security Architecture, Security Awareness, Security Automation sowie Datenschutz.

Unser fachkundiges Expertenteam, das über eine langjährige einschlägige Beratungserfahrung verfügt, hat bereits über 100 Kundenprojekte in den Branchen Telekommunikation, Logistik, Finanzdienstleistungen, Gesundheitswesen und Energie erfolgreich umgesetzt.

UNSERE STANDORTE

Standort Essen

carmasec GmbH & Co. KG
Ruhrallee 185
45136 Essen

Standort Köln

carmasec GmbH & Co. KG
Im Mediapark 5
50670 Köln