ALARM
Awareness Labor KMU Informationssicherheit

Niederschwelliges Sicherheitskonzept zum Thema Passwörter

für Geschäftsführung und IT-Verantwortliche

Thinking Objects GmbH

Stand: Mai 2023

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Das vorliegende **niederschwellige Sicherheitskonzept für KMU** ist eines von insgesamt sieben Sicherheitskonzepten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ der Technischen Hochschule (TH) Wildau verfasst werden.

Das Projekt „ALARM Informationssicherheit“ wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert.

Projektlaufzeit

01.10.2020 – 30.09.2023

Das niederschwellige Sicherheitskonzept für KMU basiert auf Ergebnissen der im Projekt „ALARM Informationssicherheit“ durch den Unterauftragnehmer Thinking Objects (TO) GmbH in Pilotunternehmen durchgeführten „Vor-Ort-Angriffen“.

Das diesem Sicherheitskonzept zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Inhaltsverzeichnis

1 Einleitung

Das Thema Passwörter beschäftigt Anwenderinnen und Anwender sowie und IT-Verantwortliche schon seit langem. Zum einen sind sie sicherheitsrelevant, zum anderen irgendwie auch lästig.

Aber warum sind sie so wichtig? Wenn ich das Passwort einer Person kenne, kann ich ihre digitale Identität übernehmen. Ich kann in ihrem Namen alles tun, was ich will. Im Nachhinein muss die Person abstreiten und beweisen, dass sie nicht selbst die Tätigkeiten, wie zum Beispiel eine Anmeldung am System, einen Post in einem Forum oder ähnliches durchgeführt hat. Das trifft sowohl auf die private Identität als auch die Identität im Unternehmen zu. Bei letzterem hat auch das Unternehmen eine zwingende Notwendigkeit, die korrekte Identität der Mitarbeiterin oder Mitarbeiters sicherzustellen.

Der Anmeldename sagt einem System, welcher Anwender oder welche Anwenderin das System nutzen will. ist. Um einem System zu beweisen, dass man wirklich dieser Benutzer oder diese Benutzerin ist, teilt man ein Geheimnis mit dem System: das Passwort. Kann man dem System dieses Passwort nennen, bestätigt einem das System diese Identität. Erfährt jemand anders von diesem Geheimnis, kann er dem System vorspielen, der „echte“ Anwender oder die echte Anwenderin zu sein. Darum ist der Schutz dieses Geheimnisses so wichtig.

2 Identitäten und Passwörter

Mit dem Passwort weise ich dem Computer-System oder dem Web-Service gegenüber nach, dass ich die Person bin, zu der der Account gehört.

2.1 Wie funktioniert das mit den Passwörtern?

Das Passwort ist ein Geheimnis, das nur ich kennen sollte und sonst niemand. Auch das Computer-System kennt normalerweise nicht dieses Passwort, sondern nur das Ergebnis einer komplexen mathematischen Operation mit diesem Passwort. Damit schützt ein Computer-System das Geheimnis. Jedes Mal, wenn ich mich anmelde, führt der Computer diese mathematische Operation mit meiner Eingabe durch. Stimmt das Ergebnis mit dem gespeicherten Ergebnis überein, glaubt der Computer, dass ich der berechtigte Benutzer oder die Berechtigte Benutzerin der Identität bin.

Aus dem vom Computer gespeicherten Wert ist das Geheimnis, also meistens das Passwort, nicht trivial rückwärtszuberechnen. Für Angreiferinnen oder Angreifer ist dieser gespeicherte Wert nicht völlig nutzlos, wenn darauf zugegriffen und der Wert kopiert werden kann. Damit kann versucht werden, das Passwort durch Ausprobieren zu erraten. Diese Versuche werden auf den eigenen Systemen der Angreifenden durchgeführt, somit werden diese Rateversuche auf den ursprünglichen Systemen nicht festgestellt.

Für diese Rateversuche nutzen Angreifende Wörterbücher, Listen mit gängigen Passwörtern oder Informationen aus sozialen Netzwerken, um daraus Passwörter abzuleiten, die gegen den gespeicherten Wert geprüft werden.

Was bringt es uns für die Verteidigung, nicht das Passwort, sondern den errechneten Wert abzuspeichern? Zeit. Wir gewinnen Zeit, den Zugriff auf den gespeicherten Wert zu erkennen und beispielsweise die Passwörter zu ändern.

2.2 Was ist ein gutes Passwort?

Ein gutes Passwort ist nicht leicht zu erraten, weder von den Bösen noch von den Guten. Im Optimalfall kann sich der Bewahrer des Geheimnisses dieses Geheimnis gut merken. Diese Anforderungen, schwierig zu erraten aber einfach zu merken, erzeugen die bekannten Schwierigkeiten, die wir mit Passwörtern haben.

Im Folgenden geht es um die Passwörter, die man sich merken muss, um sich am Arbeitsplatz-PC oder zuhause am privaten Computer anzumelden.

Für ein gutes Passwort gibt es zwei Hauptkriterien: Länge und Komplexität.

So bilden es auch die aktuellen Richtlinien und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) ab.

Ansatz 1: ein langes und wenig komplexes Passwort

Für ein Passwort dieser Art verwenden sie eine Aneinanderreihung von Worten, gerne auch getrennt durch Sonderzeichen oder Zahlen. Ziel ist es, mindestens eine Länge von 25 Zeichen zu erreichen, dafür darf der Einsatz von besonderen Zeichen reduziert werden.

Beispiel: tisch!himmel!kenia!blau!pfannkuchenteig!lachen

Ansatz 2: ein kürzeres und komplexes Passwort

Für ein Passwort dieser Art verwenden sie alle vier Zeichenarten (Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Zahlen) um eine hohe Komplexität zu erreichen.

Beispiel: x§uP3?e0aA

Wer es schafft, eine Kombination aus beidem zu verwenden, also ein langes und komplexes Passwort bildet, erreicht ein deutlich höheres Schutzniveau.

Die hier beschriebenen Möglichkeiten versuchen, Angreifenden das Erraten der Passwörter möglichst zu erschweren. Die Benutzerinnen und Benutzer müssen jedoch selbst entscheiden, welche Methode persönlich die besser geeignete ist, um sich ein Passwort zu merken.

2.3 Was ist ein gutes Passwort?

Schlechte Passwörter sind zu kurz, bestehen einfach nur aus einem Wort aus dem Wörterbuch, egal welcher Sprache oder bestehen aus einem Wort und zwei oder drei angehängten Ziffern. Auch (Kose-)Namen sind keine besseren Passwörter. Ein Passwort wird schlecht, wenn es mit anderen Benutzern geteilt wird.

Menschen denken häufig, dass etwas, was sie sich schwierig merken können von einem Angreifer nicht erraten werden kann. Das ist leider falsch, da sich die Angreifer zum einen technischer Hilfsmittel bedienen und zum anderen auf sehr viele Quellen für mögliche Passwörter (Wörterbücher, Wortlisten, bekannte Passwörter, etc.) zurückgreifen können.

2.4 Wie verwende ich Passwörter?

In besten Fall teile ich mit jedem Computer-System und Internet-Angebot ein eigenes Geheimnis. Das bedeutet, ich habe überall ein anderes Passwort. Warum sollte das so sein? Wenn Angreifende in der Lage sind, ein Passwort zu stehlen und oder den gespeicherten Wert zu entschlüsseln, dann werden sie dieses Passwort überall im Internet ausprobieren. Da in der Regel überall die E-Mail-Adresse als Kennung eingesetzt wird, kann das an vielen Diensten ausprobiert werden.

Das gilt sowohl für firmenbezogene als auch private Accounts. Hilfreich in diesem Zusammenhang ist ein Passwort-Manager, also eine Software, die alle Passwörter sicher verwahrt; mehr dazu im nächsten Kapitel.

2.5 Wie merke ich mir all die Passwörter?

So viele Passwörter wie Internet-Dienste existieren kann sich kein Mensch merken. Darum ist ein Einsatz eines Passwort-Managers zu empfehlen.

In einem **Passwort-Manager** trage ich alle Dienste und Systeme mit der Anmelde-Kennung und dem Passwort ein. Im Idealfall kenne ich das Passwort nicht, sondern habe es nur im Passwort-Manager generiert und gespeichert. Ob ich ein 12 Zeichen langes Passwort aus dem Passwort-Manager kopiere oder ein 24 Zeichen langes und komplexes Passwort ist für mich als Anwender völlig unerheblich, aber einen Hacker erschwert es das Knacken des Passwortes deutlich.

Darum können auch alle Passwörter im Passwort-Manager zufällig mit einer Länge von 20 Zeichen oder mehr generiert werden.

Das bedeutet am Ende ich muss mir nur wenige Passwörter merken:

- Das Passwort für den Unternehmens PC
- Das für den Passwort-Manager im Unternehmen.
- Das für den privaten PC
- Das für den privaten Passwort-Manager

Mit diesen vier Passwörter kann ich alles erledigen. Alle anderen Passwörter kann ich in einem Passwort-Manager speichern und brauche sie eigentlich auch gar nicht mehr zu wissen.

Das Speichern von Passwörtern in der Software, beispielsweise im Browser, birgt die Gefahr, dass nach Neuinstallation oder bei Verwendung eines anderen Browsers, das Passwort nicht mehr bekannt ist. Darum sollten Passwörter immer im Passwort-Manager gespeichert werden, im Browser oder anderen Applikationen dürfen sie aber zusätzlich gespeichert werden.

2.6 Wie funktioniert Passwort-Diebstahl?

Angreifern und Angreiferinnen können Passwörter in verschiedenen Arten in die Hände fallen.

Im einfachsten Fall kann das Passwort im Klartext abgegriffen werden. Der gängige und häufig praktizierte Weg hierfür ist Phishing. Dafür wird den Benutzern und Benutzerinnen eine täuschend echte Anmeldeseite eines Internet-Dienstes vorgegaukelt, in die die eigenen Anmeldedaten eingeben werden sollen. Da es sich um eine gefälschte Seite der Angreifenden handelt, steht ihnen nun eine Kombination aus Login und Passwort zur Verfügung. Eine andere Variante kann beispielsweise der Einsatz einer Schadsoftware in Form eines Virus oder eine Malware sein. Ist ein Rechner oder Smartphone von einer solchen Malware befallen, kann sie Tastureingaben protokollieren und an die Angreifenden schicken.

Gelingt es den Angreifenden einen Internet-Service zu hacken, bei dem die Anwenderin oder der Anwender einen Account hat, gelangen sie in der Regel nur in den Besitz der gespeicherten Werte. Diese kann er bei korrekter Implementierung nicht direkt entschlüsseln. Er muss seine sogenannten Wortlisten durchprobieren, ob eines davon den gespeicherten Wert ergibt. Ist das der Fall, hat er nun ebenfalls ein Passwort, das funktioniert. Zur üblichen Vorgehensweise dieser Tools gehört es auch, Zahlen an die Passwörter anzuhängen, so dass aus einem Wort der Wortliste schnell tausende von Varianten werden, die im Bruchteil einer Sekunde durchprobiert werden können.

Diese vollständigen Account-Daten werden dann oftmals auch im sogenannten Darknet zum Kauf angeboten, somit erweitert sich der Kreis der möglichen Angreifenden, die mit dem ursprünglichen Passwort-Diebstahl nichts zu tun hatten, aber die Accounts nun für ihre Zwecke nutzen können.

Dass Angreifende tatsächlich vor einer Eingabemaske sitzen und versuchen, ein Passwort zu erraten, kommt praktisch nicht vor. Vielmehr sind solche Angriffe fast vollständig automatisiert und daher sehr viel wirkungsvoller als eine menschliche Eingabe.

2.7 Wie bekomme ich mit, dass mein Passwort gestohlen wurde?

Hier hilft nur der sorgsame und bewusste Umgang mit Passwörtern. Es gilt, wachsam zu sein.

Es gibt Dienste, die versenden E-Mails bei jeder erfolgten Anmeldung, oder sie stellen ein Protokoll der letzten erfolgreichen Anmeldungen zur Verfügung. Manchmal melden die Dienste bei einer Anmeldung auch, wann die letzte Anmeldung erfolgte. Wenn diese zu unüblichen Uhrzeiten, beispielsweise Mitten in der Nacht, oder von unüblichen Orten, beispielsweise anderen Kontinenten, erfolgen, ist in der Regel von einem Verlust des Passwortes auszugehen.

Zusätzlich kann man über Dienste wie **haveibeenpwned** und den **HPI-Identiy Checker** prüfen lassen, ob beispielsweise Accountdaten bei einem Internet-Dienst gestohlen wurden. Ist die E-Mail-Adresse hier entsprechend gelistet, besteht zumindest ein Risiko, dass das Passwort in fremde Hände gerät.

Anwender und Anwenderinnen, die Passwörter immer individuell und/oder zufällig erzeugen, sind hier im Vorteil. Hierbei können Angreifende die gewonnen Informationen nicht direkt zur Verwendung mit weiteren Accounts nutzen.

2.8 Wann muss ich mein Passwort ändern?

Das Passwort muss immer dann geändert werden, wenn der Verdacht oder die Gewissheit besteht, dass es in fremde Hände geraten ist.

Dann sollte das Passwort auch entsprechend vollständig geändert werden und nicht beispielweise eine neue Zahl angehängt oder ein Sonderzeichen ausgetauscht werden.

Wer auf Nummer sicher gehen will, ändert sein Passwort in regelmäßigen Abständen, um bei einem Diebstahl nicht von den oben genannten Warnzeichen abhängig zu sein. Aber auch hier gilt: ein völlig neues Passwort erfinden, keine Variation mit ausgetauschten Zeichen und Ziffern.

2.9 Was ist Zwei-Faktor-Anmeldung?

Viele Dienste bieten mittlerweile eine Zwei-Faktor-Anmeldung an, viele Unternehmen schreiben es vor. In der Regel wird sie überall dort verwendet, wo eine Anmeldung aus dem gesamten Internet möglich ist. Bei der Zwei-Faktor-Anmeldung handelt es sich in der Regel um ein weiteres Merkmal zusätzlich zum Geheimnis, um die Benutzerinnen und Benutzer zweifelsfrei identifizieren zu können. In der einfachen Variante sind das sogenannte Tokens, die zeitbasiert funktionieren, und zusätzlich als Nummernfolge eingegeben werden müssen. Ohne den passenden Token können die Angreifenden sich nicht mit dem gestohlenen Passwort anmelden. Da dieser Token nur kurz gültig ist (in der Regel 30 oder 60 Sekunden), kann er auch nicht durch Probieren erraten werden.

Für den Anwender oder die Anwenderin wird die Anmeldung komplizierter, darum gibt es mittlerweile komfortable Varianten dieses Verfahrens. Die sogenannte Multi-Faktor-Anmeldung zieht weitere Kriterien in Betracht, ob der zusätzliche Token abgefragt wird. Ungewöhnliche IP-Adressen, neue Browser oder Rechner führen im Prinzip zur Abfrage des zweiten Faktors. Wie der zweite Faktor nun aussieht, ist ebenfalls viel dynamischer. In den meisten Fällen für Unternehmen handelt es sich um eine App auf dem Smartphone, die entweder einen Code zur Eingabe bereitstellt oder nur auf eine Bestätigung durch die Anwenderin oder den Anwender wartet.

Die Nutzung eines privaten Smartphones als zweiten Faktor auch im Unternehmensumfeld ist in jedem Fall besser als keinen zweiten Faktor zu verwenden. Eine entsprechende Betriebsvereinbarung oder Richtlinie ist hierbei zu empfehlen.

2.10 Was ist passwortlose Anmeldung?

Passwortlose Anmeldung ist ein von Microsoft, Apple und Google definiertes Ziel, die lästigen Passwörter abzuschaffen. Basis hierfür ist der FIDO 2 Standard sowie zusätzliche Geräte wie Smartphones oder USB-Tokens, die für die Anwender einen Besitz darstellen. Sicher funktionieren kann das alles nur wenn das Geheimnis auf dem Gerät nicht aus diesem extrahiert werden kann, beispielsweise weil das Geheimnis innerhalb eines sicheren Chips erzeugt wird und niemals aus diesem Chip ausgelesen werden. Nur in diesem Fall kann die passwortlose Anmeldung auch als sicher betrachtet werden. Denn wenn eine Kopie mit dem identischen Geheimnis ohne Wissen des Benutzers erzeugt werden kann, dann nutzt der Besitz des Gerätes nicht, weil der Verlust nicht bemerkt werden kann.

Der Zugriff wird in der Regel zusätzlich noch über PINs oder biometrische Merkmale (Fingerabdruck) geschützt, um eine angemessene Reaktion bei Verlust zu ermöglichen.

Technische Hochschule Wildau
Technical University of Applied Sciences

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770400
Fax. +49 711 88770449
www.to.com