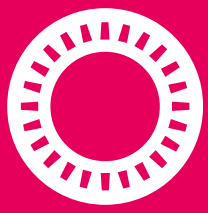


MATESO
PASSWORD SAFE

Sicherheitslücke Mensch

Inhaltsverzeichnis

Einleitung

Der Kampf um mehr Cybersicherheit ist ein fortlaufender Prozess ohne Verschnaufpause. Von Deepfakes bis hin zu gefälschten Websites: Im Zuge der Digitalisierung rüsten auch Hacker auf und wirken stets einen Schritt voraus in der Entwicklung neuer Angriffsszenarien. Bei der wachsenden externen Bedrohungslage wird gerne ein wichtiger Faktor übersehen – die Gefahr vor dem PC: Der eigene Mitarbeiter stellt ein enormes Sicherheitsrisiko für Unternehmen dar – ob bewusst oder unbewusst spielt dabei erst einmal keine Rolle. Laut aktuellen Studien sehen 76 % der Befragten schlecht geschulte Mitarbeiter als größtes Sicherheitsrisiko für Unternehmen. Fakten wie diese, dass jeder zweite sein Passwort für eine Tafel Schokolade verraten würde, sind dabei so schockierend wie real.

Dieses Whitepaper soll deshalb als Informationsgrundlage für Unternehmen dienen, um die eigenen Mitarbeiter als Risikofaktor besser einschätzen zu lernen und dahingehend Schutzmaßnahmen zu entwickeln.

> **Es gibt keine Sicherheit, nur verschiedene Grade der Unsicherheit.**
>
> **Anton Neuhäusler,** Professor für Philosophie

Risiko-Szenarien

Betrachtet man den Menschen als Sicherheitslücke der Cybersicherheit, entstehen zwei Dimensionen – die bewusste sowie die unbewusste Beschädigung interner Sicherheitsmechanismen. Bewusster Datenmissbrauch entsteht meist aufgrund von kriminellen Absichten, Unzufriedenheit oder aus wirtschaftlichem Interesse. Der unbewusste Missbrauch von Daten hingegen geschieht durch Unachtsamkeit oder mangelndes Know-how und Ressourcen.

Die daraus entstehenden Folgen können auf beiden Seiten enorm sein – finanziell als auch durch das Erleiden eines Reputationsverlustes nach außen. Obwohl jeder Datenmissbrauch individuell unterschiedlich ist, lassen sich allgemeine Szenarien skizzieren, um daraus Muster abzuleiten und Lösungsszenarien zu entwickeln.

Bewusster Datenmissbrauch

Spionage und Diebstahl von internen Informationen und Geheimnissen

Nicht jeder Austritt eines bestehenden Mitarbeiters verläuft so harmonisch wie gewollt: Gehen beide Parteien nicht in Frieden auseinander, sind die internen Daten theoretisch gefährdet. Denn Mitarbeiter können diese kopieren, um sie dem neuen Arbeitgeber oder auch Konkurrenzunternehmen zur Verfügung stellen oder sie zum Start in die Selbstständigkeit nutzen.

Willkür im Umgang mit sensiblen Daten

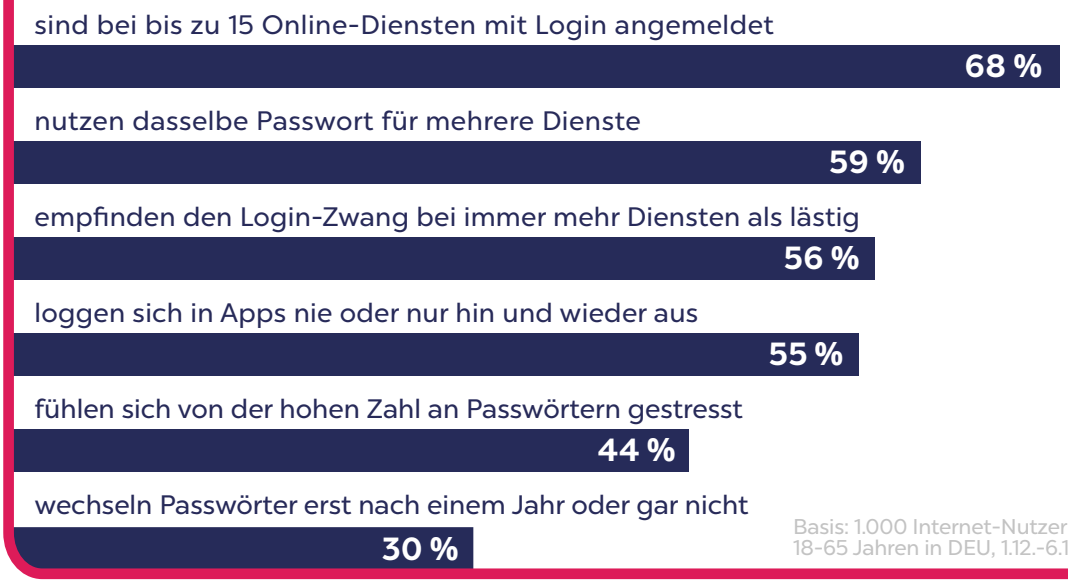
Auch Mitarbeiter, die keine Zukunft im Unternehmen sehen, könnten nachlässig mit den internen Daten und Geheimnissen umgehen. Dies äußert sich zum Beispiel im achtlosen Umgang mit Passwörtern, dem Besuch von unsicheren Websites oder dem potentiellen Download von Schadsoftware. Auch kann es passieren, dass Mitarbeiter Daten und Accounts löschen.

Datenveruntreuung und Sabotage

Im Extremfall können sich Mitarbeiter dazu entschließen, die interne IT-Infrastruktur bewusst anzugreifen und lahmzulegen, um so einen finanziellen Schaden zu provozieren oder das Unternehmen zu erpressen. Da der Mitarbeiter Zugriff von innen hat, ist es für ihn auch ein Leichtes, mit Hackern zusammenzuarbeiten und ihnen Zugriff zu allen Daten zu gewähren. Laut Bitkom wurde bereits jedes zweite Unternehmen Opfer von Datenmissbrauch wie Sabotage.

Passwort-Fakten[1]

Befragte Internet-Nutzer zu Ihrem Umgang mit Passwörtern



Basis: 1.000 Internet-Nutzer von 18-65 Jahren in DEU, 1.12.-6.12.2016.

Unbewusster Datenmissbrauch

Unsachgemäßer Gebrauch von Passwörtern

Besitzen Mitarbeiter wenig Sensibilität im Umgang mit sicherheitsrelevanten Daten und Zugängen, ist der achtlose Umgang mit Passwörtern meist die Folge. Passwörter werden im Klartext geteilt, auf Zettel geschrieben und weitergegeben und an unsicheren Orten wie Excel-Listen gespeichert. Dieses Vorgehen kann bereits einen Verstoß gegen den Datenschutz darstellen, worüber sich die Mitarbeiter meist nicht im Klaren sind. Zudem werden in Eigenregie Registrierungen für neue Anwendungen und Websites vorgenommen und für die jeweiligen Zugänge unsichere oder schon verwendete Passwörter genutzt.

Besitzt der Mitarbeiter kein Gespür für mehr Sicherheitsbewusstsein, können auch Sicherheitsrichtlinien falsch umgesetzt werden, sodass diese dem Unternehmen sogar mehr schaden als nutzen können. Wird Mitarbeitern, die sich Passwörter im Kopf merken, etwa ein regelmäßiger Austausch dieser empfohlen, greifen sie gerne nur zu leicht abgewandelten Versionen der bereits existierenden Passwörter, indem sie sie leicht abändern oder mit Sonderzeichen und Ziffern erweitern.

Diese Muster sind für Hacker ein typisches Vorgehen, weshalb solche Passwörter besonders leicht durchschaut und schnell geknackt werden können.

Folgende Angriffsmethoden werden dadurch begünstigt:

Password Spraying

Bei dieser Attacke wird versucht, mit wenigen, häufig verwendeten Passwörtern auf eine große Anzahl von Konten / Benutzernamen zuzugreifen. Verwendet der Mitarbeiter also ein allgemein geläufiges Passwort und/oder ein Passwort für mehrere Konten, steigt das Risiko, durch Password Spraying gehackt zu werden.

Dictionary Attacks

Auch logische Kombinationen oder Wörter, die in Wörterbüchern zu finden sind, stellen für Hacker keine Herausforderung dar. Durch so genannte Dictionary Attacks wird ein unbekanntes Passwort mithilfe einer Passwortliste ermittelt. Verwendet der Mitarbeiter also ein Passwort, das so auch (teilweise) im Wörterbuch zu finden ist, steigt das Risiko erheblich, gehackt zu werden.

Download / Installation von Schadware

Ist ein Mitarbeiter ahnungslos über Risiken, können Schadware-Programme – etwa durch Klick auf den falschen Link – leicht Zugang in Unternehmen finden. Eine bewusste Installation des Programms ist hierbei nicht einmal mehr notwendig, da sich Viren und Co. selbstständig im System festsetzen und der Schaden automatisiert seinen Lauf nimmt.

Spezielle Überwachungsprogramme können nicht gewünschte Downloads und/oder Installationen dokumentieren und auch blockieren. Dazu gehören immer Präventionsmaßnahmen im Sinne von Awareness Trainings, um im Vorfeld den Klick auf einen gefährlichen Link als Risiko ausklammern zu können.

Falscher Umgang mit Datensicherheits-Vorfällen

Um bei einem Verstoß gegen die internen Sicherheitsrichtlinien richtig agieren zu können, müssen die entsprechenden Sicherheitsverantwortlichen in erster Linie erst einmal Kenntnis darüber erlangen. Vertuscht der Mitarbeiter etwa einen Vorfall aus Scham oder ist ihm der Verstoß gar nicht bewusst, können die Parteien auch nicht präventive oder reaktive Maßnahmen einleiten.

Auch wenn überhaupt kein interner Maßnahmenkatalog implementiert ist, sind Mitarbeiter teilweise unsicher, an wen sie sich wann wenden können. Für eine zweiseitige gesunde Kommunikation ist zudem ein positives Betriebsklima essentiell, um die Hemmschwelle bei den Mitarbeitern zu senken, Sicherheitsvorfälle aufzudecken.

Social Engineering

Social Engineering, auch Social Hacking genannt, beschreibt die Vorgehensweise, durch Täuschung und Manipulation menschliche Eigenschaften wie Gutgläubigkeit, Hilfsbereitschaft und Unsicherheit auszunutzen, um an sicherheitstechnisch relevante Daten zu gelangen oder Schadware zu installieren.

Phishing

Unter Phishing (angelehnt an die englische Bedeutung von fishing: Angeln) werden Versuche gezählt, über gefälschte Websites, E-Mails und/oder Kurznachrichten an persönliche Daten zu gelangen. Durch Phishing können leicht Kontoplünderungen begangen werden, indem der User seine Kontoinformationen auf einer gefälschten Website eingibt, auf die er durch Klick auf den Link in einer täuschend echten E-Mail seines Bankanbieters wie der Postbank weitergeleitet wurde.

Aus Phishing können weitere Angriffsszenarien abgeleitet werden:

Spoofing

Unter Spoofing versteht man das Vortäuschen einer anderen Identität, um in den PC oder Netzwerke einzudringen. Dabei werden meist IP und/oder Adresse so gefälscht, dass der Empfänger sie für vertrauenswürdig hält und daraufhin auf den enthaltenen Link klickt oder den Anhang öffnet. Als Folge können Malware oder Keylogger unbemerkt auf dem System installiert werden.

Um Spoofing zu verhindern, sollten Mitarbeiter immer wieder dazu aufgefordert werden, verdächtige E-Mails zu melden und sich lieber Expertenrat einzuholen, wenn Unsicherheit über deren Vertrauenswürdigkeit besteht. Werden die Login-Informationen in einem Password Manager gespeichert, erübrigt sich sogar das Problem: Denn da die enthaltenen Login-Daten wie die IP-Adresse zur automatischen Anmeldung dort hinterlegt sind, erkennt der Password Manager gefälschte Adressen und verhindert den Login erfolgreich. So merkt der Mitarbeiter trotz Klick auf den Link noch rechtzeitig, dass er es mit einem falschen Link zu tun hat.

Pharming

Pharming ist eine weiterentwickelte Methode des Phishings, indem gezielt Domain-Name-System-Anfragen (kurz: DNS-Anfragen) an den Webbrowser manipuliert werden. Mithilfe von DNS werden Web-Adressen in IP-Adressen umgewandelt. Wird nun etwa eine Zahl der IP-Adresse in der Host-Datei verändert, wird der User trotz richtiger Eingabe der Webadresse auf die gefälschte Seite weitergeleitet, ohne es zu merken. Beim Pharming ist also nicht einmal der Klick auf einen falschen Link zur Täuschung notwendig. Gibt der User nun seine vertraulichen Daten auf der gefälschten Seite ein, ist das Pharming erfolgreich abgeschlossen.

Um Pharming zu verhindern, sollte bei Eingabe der Adresse stets mit „https://“ begonnen werden. Auch kann eine Authentifizierung des Servers durch automatischen Austausch eines Zertifikates abgefragt werden. Ein aktuelles Virenprogramm sowie eine gute Firewall sind essentiell, um Pharming entgegenzuwirken.

Deepfakes

Durch künstliche Intelligenz werden auch Phishing-Attacken auf ein neues Level gehoben. Denn KI ermöglicht es Angreifern, ihre Opfer noch besser zu täuschen. Vor allem Deepfakes sind hier zu nennen – abgeleitet aus den Begriffen Deep Learning und Fake. Deepfakes ermöglichen es den Angreifern, Medieninhalte wie Bilder, Videos oder Audio-Dateien mithilfe von KI und Machine Learning zu manipulieren, um die Opfer hineinzulegen.

Mittlerweile sind Deepfakes sogar so ausgereift, dass die Kopie kaum noch vom Original zu unterscheiden ist. Es könnte also ohne weiteres die Stimme des CEOs am Telefon perfekt nachgeahmt werden, der den Mitarbeiter bittet, ihm unverzüglich eine gewisse Summe auf jenes Konto zu überweisen.

Da Deepfakes noch eine relativ neue Methode darstellen, sind Schutzmechanismen noch schwer zu definieren. Fakt ist, dass sie die Notwendigkeit von Awareness Trainings noch weiter in den Vordergrund rücken, damit Mitarbeiter lernen, Handlungen zu hinterfragen und auch auf eher unbekannte Taktiken besser vorbereitet sind.

Shoulder Surfing

Nicht auf die leichte Schulter zu nehmen ist das sogenannte Shoulder Surfing. Hierbei schaut der Täter dem Opfer sprichwörtlich über die Schulter, während dieser zum Beispiel sein Passwort eingibt. Gerade in der Öffentlichkeit kann es passieren, dass etwa in der Bahn geheime Informationen mitgelesen und daraufhin entwendet werden. Diese eher einfach anmutende Methode ist gleichermaßen effizient für den Täter, da er keinerlei technisches Know-how benötigt, um an Passwörter oder PIN-Codes zu gelangen.

Mitarbeiter sollten deshalb immer wieder darauf hingewiesen werden, sensible Daten verdeckt einzugeben – vor allem unterwegs. Blickschutzfilter und -folien sorgen zudem dafür, dass Dritten eine Sicht auf den Bildschirm erschwert wird. Ist ein Password Manager in Verwendung, kann festgelegt werden, dass Passwörter nur verdeckt via Single-Sign-on eingetragen werden können. Auch ein zweiter Faktor ist hilfreich, da dieser sich jedes Mal ändert oder dem Angreifer nicht zur Verfügung steht.

Security Awareness als Lösung

An erster Stelle steht, ein Sicherheitsbewusstsein bei jedem einzelnen Mitarbeiter zu generieren. Security Awareness bedeutet, dass der Mitarbeiter aktiv zum Schutz des Unternehmens beiträgt, da seine Einstellung dazu, sein dazugehöriges Wissen als auch seine damit einhergehenden Handlungen mit den internen Datensicherheitsrichtlinien konform sind.

Dieses Bewusstsein kann durch Schulungen und Trainings als auch durch spezifische Kampagnen erwirkt werden. Wichtig dabei ist, dass Sicherheitsmaßnahmen von jedem Mitarbeiter verstanden und leicht umgesetzt werden können und dabei ihr individueller technischer Wissensstand berücksichtigt wird.

Standardisierte Prozesse und Dokumente

Jedem Mitarbeiter muss bewusst sein, an welchen Ansprechpartner im Unternehmen er sich wenden kann, wenn er Fragen zur IT-Sicherheit hat oder es zu einem Sicherheitsvorfall gekommen ist und wie dazu vorgegangen wird. Entsprechende Unterlagen müssen jedem Mitarbeiter leicht zugänglich sein, damit dieser sich selbst auf dem aktuellen Stand halten und über neueste Änderungen und Informationen informieren kann.

Inhaltliche Punkte zur Schaffung eines Sicherheitsbewusstseins:

- Cybergefahren sind allgegenwärtig und können jedes Unternehmen sowie Privatperson treffen.
- Die Komplexität als auch Stärke von Cyberangriffen nimmt exponentiell zu.
- Cybersicherheit betrifft jeden Mitarbeiter – unabhängig von seiner Position und Abteilung - nicht nur den IT-Sicherheitsbeauftragten oder den System-Administratoren.
- Der entstandene Schaden kann nicht nur finanzieller Natur sein, sondern auch einen Imageschaden und Reputationsverlust bedeuten.
- Dabei können nicht nur sensible Unternehmensdaten, sondern auch persönliche Informationen des einzelnen Mitarbeiters hier offengelegt werden.
- Sicherheitsvorfälle müssen unmittelbar gemeldet werden, um den Schaden einzugrenzen.
- Bei fahrlässigem Handeln oder nachweisbar absichtlichem Datenmissbrauch kann auch der Mitarbeiter vom Unternehmen zur Verantwortung gezogen werden.

Sicherheitsbewusstsein als fortwährende Entwicklung

Unternehmen muss klar sein, dass sich ein Sicherheitsbewusstsein nicht von heute auf morgen oder durch einmalige Schulungen einführen lässt. Die Betreuung und Rückversicherung der einzelnen Mitarbeiter sind essentiell, um Sicherheitsstrukturen langfristig umzusetzen. Beide Parteien lernen hierbei im gegenseitigen Austausch voneinander.

Interne Audits unterstützen hierbei, um einen Überblick zu erhalten, was gut funktioniert und wo nachjustiert werden muss. Durch regelmäßige anonyme Umfragen und/oder Feedbackgespräche kann beispielsweise eruiert werden, welche Punkte noch offen oder lückenhaft sind und bei welchen Prozessen sich Mitarbeiter in der Umsetzung noch unsicher sein könnten. So können Strukturen immer wieder an die Bedürfnisse der Mitarbeiter angepasst werden, um sicherzustellen, dass diese zeit- und aufwandstechnisch auch realistisch sind.

Information Security Awareness

Auch müssen Mitarbeiter als Schlüsselrolle bei der Einhaltung von Sicherheitsrichtlinien immer wieder bestärkt und bekräftigt werden. Durch interne Rundmails, Security Newsletter, eine Guideline oder visuell aufbereiteten Maßnahmen wie Plakate fühlen sich Mitarbeiter bei der Umsetzung nicht alleine gelassen, indem das Thema immer wieder in den Vordergrund gerückt wird.

Fazit

Schlussendlich lässt sich sagen, dass die Sicherheitslücke Mensch bestmöglich durch ein Verständnis über etwaige Risiken und eine gesunde interne Kommunikation ausgeklammert werden kann. Der Weg zu mehr Security Awareness lässt sich dabei für Unternehmen nicht pauschal definieren, sondern muss je nach Kenntnisstand, Motivation und Umsetzungsmöglichkeiten für die eigenen Mitarbeiter individuell entschieden werden.

Die jeweiligen Anforderungen unterscheiden sich hierbei in Abhängigkeit von gesetzlichen Vorgaben, der Größe als auch der Branche des Unternehmens. Unter Berücksichtigung aller in diesem Whitepaper genannten Faktoren kann jedoch jedes Unternehmen zu einer stabileren internen Sicherheitsinfrastruktur beitragen, indem es dem Menschen die hierfür notwendige Aufmerksamkeit zukommen lässt.

Autor:
Kristina Kaya
Product Marketing Managerin

Quellenverzeichnis:

[1] Statista 2020: Web.de, der große Passwort-Stress

[2] Statista 2019: Online-Umfrage der VDE Bayern

[3] Bitkom Studienbericht 2018: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie

MATESO

Die MATESO GmbH ist ein führendes deutsches IT-Unternehmen, das sich seit der Firmengründung in 2006 erfolgreich im DACH-Raum etabliert hat. Die entwickelte Passwort-Sicherheitslösung Password Safe wird durch ihr weltweites Partnernetzwerk international vertrieben. Namhafte Referenzen bezeugen den Technologie- und Know-how-Vorsprung der IT-Software.

Heute verzeichnet das stetig wachsende Unternehmen branchenübergreifend über 10.000 Firmenkunden mit mehreren Millionen Anwendern weltweit – darunter 20 Firmen der Dax 30.

PASSWORD SAFE

Pioneer im Enterprise Password Management

Password Safe dient Unternehmen als zentraler digitaler Tresor zur Sicherung, Verwaltung und Überwachung von sensiblen Daten wie Passwörtern, Dokumenten und Geheimnissen.

Im Umgang mit Passwörtern ist der Mensch noch unerlässlich.

Sicher ist: Alle Fehler, die er machen kann, werden gemacht.

Thomas Malchar
CEO der MATESO GmbH

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.de
Email: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE