Wie man eine positive Passwort-Kultur im Unternehmen einführt

MATESO
PASSWORD SAFE

How to Guide

Wenn Ihr Sicherheitskonzept am Mitarbeitenden vorbeigeht

Ihr Sicherheitskonzept ist aufgesetzt und einsatzbereit? Die Dienstanweisung wurde per Mail versandt und alle Ihre Mitarbeitenden „sollten nun eigentlich wissen“, wie sie mit ihren Passwörtern und der Sicherheit insgesamt umgehen sollen? Sind Sie sicher? Und sind Sie sicher, dass alle Passwörter Ihres Unternehmens sicher sind? Das können Sie wahrscheinlich nicht hundertprozentig sagen. Denn laut Bitkom verwendet jeder dritte Online-Nutzer dasselbe Passwort für mehrere Dienste. Das sind schlechte Angewohnheiten, die sich nicht so einfach abstellen lassen. Wie kann Ihr Unternehmen also langfristig mehr Sicherheitsbewusstsein entwickeln?

Was nicht funktioniert

Wussten Sie, dass Cyberattacken und Co. für Ihre Mitarbeitenden nicht so schockierend sind, wie Sie es vielleicht erwarten würden? Sicher, im ersten Moment mögen News über Sicherheitsvorfälle noch schockierend sein. Doch die Attacken häufen sich immer mehr und Nachrichten über geknackte Passwörter gehören fast schon zum Alltag für uns. Durch die Gewöhnung an derlei Vorfälle wird eine abschreckende Wirkung immer schwieriger und reicht kaum noch aus, um für eine langfristige Verbesserung des Sicherheitsverhaltens zu sorgen. Trotzdem wird Mitarbeitenden vorgeschrieben, dieses oder jenes nicht zu tun, und die Vorgesetzten versuchen, sie mit möglichen Konsequenzen zur Umsetzung zu bewegen oder Drohkulissen aufzubauen.

„Wenn ihr auf derlei Links klickt, könnt ihr Hackern gleich unsere Tür öffnen, damit sie in unser Netzwerk einzudringen und alles stehlen können.”

Beängstigend genug für einen kurzfristigen Effekt?
Denken Sie lieber voraus!

Angst als Blockierer

Warum tun sie das? Weil Angst ein starkes Gefühl ist! Indem bei den Mitarbeitenden Angst schürt, kann man aber auch das Gegenteil erreichen. Sie sind nur noch mehr verunsichert, wie sie sich in neuen und potenziell gefährlichen Situationen verhalten sollen. Diese Angst hindert sie dann daran, klar und vorausschauend zu denken. Oder Ihre Mitarbeitenden halten die Szenarien für übertriebene Panikmache und nehmen sie erst gar nicht ernst.

Ja, Angst ist ein starkes Gefühl. Aber eben auch nur kurzfristig. Sie kann Ihre Mitarbeitenden dazu bringen, ihr Passwort einmal zu ändern oder sich ein sehr komplexes Passwort auszudenken. Aber wenn die Angst verflogen ist, kehren die alten Gewohnheiten zurück. Laut einer Studie von IGS sind über 85 % der Befragten der Auffassung, dass Druck als Führungsmittel eingesetzt wird. Die Folgen daraus sind demnach weniger Leistungsbereitschaft, Engagement und Loyalität. Auf lange Sicht können Angst und Druck also eher abstumpfend auf Mitarbeitende wirken. Bei der nächsten Änderung des Passworts wird also daraufhin einfach ein Sonderzeichen hinzugefügt und so weiter ... Und die verbleibende Angst wird weiterhin als stumme Warnung mitschwingen und Ihre Mitarbeitenden daran hindern, produktiv zu arbeiten.

Wenn Mitarbeitende Angst haben, Fehler zu machen, ist das Risiko, dass es zu Fehlern kommt, gleich noch größer. Denn Angst führt zu unsicherem Verhalten. So werden sie sich beispielsweise beim Einloggen häufiger vertippen oder den sicheren Platz für ihr Passwort, den sie nach der letzten Warnung eilig ausgesucht haben, nicht mehr finden.

Denn Angst führt dazu, dass Mitarbeitende impulsiv und nicht logisch und informationsbasiert handeln. Das einfache Hinzufügen einer Zahl zu einem Passwort kann aus einem Impuls heraus geschehen, ebenso wie das schnelle Verstecken des Passworts auf einem Post-It unter der Tastatur. **Obwohl Angst also ein starkes Gefühl ist, kann sie für Ihr Unternehmen kontraproduktiv werden, wenn sie als bloßes Mittel zum Zweck eingesetzt wird.**

Richtlinien, die unerreichbar scheinen

Eine Frage, die sich Unternehmen stellen sollten: „Hat mein Mitarbeitender bereits alles, was er benötigt, um sich an die intern aufgestellten Regeln zu halten?“ Wenn es um Passwörter geht, kann es für Mitarbeitende anspruchsvoll und manchmal sogar unmöglich sein, sich an diese Regeln zu halten, wenn sie keine Hilfe oder nicht die richtigen Werkzeuge dafür zur Verfügung haben. So wird den Mitarbeitenden beispielsweise gesagt, dass sie nur eindeutige Passwörter für jedes Konto verwenden, diese alle drei Monate ändern und sie nicht aufschreiben sollen. Dabei wird oft übersehen, dass dies bei durchschnittlich 26 Passwörtern pro Mitarbeitendem viel Aufwand bedeutet. Das kann im Endeffekt dann dazu führen, dass sie aufgeben und zu Behelfslösungen wie Schatten-IT greifen. Das Problem scheint also nur vermeintlich gelöst, auf dem Weg dorthin wurde jedoch der Mensch mit seinen Bedürfnissen außer Acht gelassen. Aus diesem Beispiel wird immer deutlicher, wie wichtig die Einführung eines Modern Workplace ist, der auch die IT-Sicherheit als Grundstein von Compliance bildet und auch Tools und Prozesse zur Umsetzung bietet.

Der Mensch im Mittelpunkt
Modern Workplace als Zusammenspiel von Geräten, Technologien und Software

- Ob im Home Office oder unterwegs: verschiedene Arbeitsumgebungen ermöglichen
- Work-Life-Balance? Arbeitsbedingungen beachten
- Von Open Door bis Standup-Desk: Wohlfühl-Atmosphäre erschaffen
- Security Enablement: Tools und Services bieten

Was wirklich funktioniert

Warum machen wir das? Verständnis schaffen!

Wenn es um Regeln und Richtlinien geht, stellen wir sie oft allen Mitarbeitenden vor und sagen: „Daran werden wir uns jetzt halten, weil die Regierung / das Management / andere Richtlinien uns das vorschreiben." Wir verbringen also viel Zeit damit, unseren Mitarbeitenden zu erklären, dass dies oder jenes wichtig ist. Wir erinnern sie regelmäßig daran, sich an diese Richtlinien zu halten, und überprüfen ihr Verhalten von Zeit zu Zeit. Was aber fehlt, ist ein echtes Verständnis auf der anderen Seite. Und dabei geht es nicht darum, sie mit möglichen Konsequenzen für sich selbst oder das Unternehmen zu konfrontieren. Es geht darum, nach und nach ein Sicherheitsbewusstsein zu schaffen und sich auf das positive Ergebnis zu konzentrieren, wenn Regeln ausgerollt oder angepasst werden. „Wenn wir einem Passwort nur zwei Sonderzeichen hinzufügen, brauchen Hacker bereits x Mal mehr Zeit, um es zu knacken" oder „Wenn wir unsere Passwörter regelmäßig ändern, können wir unsere interne Passwortsicherheit um x % erhöhen": Auf diese Weise geben Sie Ihren Mitarbeitenden nicht das Gefühl, dass sie Teil der Ursache eines Problems sind, das eliminiert werden muss. **Ihre Mitarbeitenden werden Teil einer positiven Veränderung und ein aktiver und wichtiger Teil der Lösung, zu der sie durch ihr tägliches Engagement beitragen.**

Finden Sie die richtigen Argumente für Ihre Mitarbeitenden

Um eine positive Passwortkultur in Unternehmen zu leben, zählen für Mitarbeitende die richtigen Argumente. So hart es klingen mag: Ihre Mitarbeitenden werden sich weniger um die interne Passwortsicherheit sorgen als Sie selbst. Denn für diese ist Produktivität – und dazu gehört auch, sich schnell und einfach einzuloggen – wichtiger als Sicherheit. Sie haben tägliche Termine, die sie einhalten, Anrufe, die sie annehmen und Projekte, die sie abschließen müssen. Login und Co. werden höchstens nur als notwendiges Übel wahrgenommen.

Wie bringen Sie also Ihre Mitarbeitenden auf die sichere Seite? Indem Sie ihnen die Arbeit erleichtern und ihnen einen echten Mehrwert für sich aufzeigen: Wenn Ihre Mitarbeitenden Sicherheit als etwas Positives sehen, das ihnen in ihrem Arbeitsalltag tatsächlich hilft, werden sie den Nutzen erkennen und sich langfristig gerne daran beteiligen. Aus diesem Grund sollte Sicherheit als Enabler und nicht als Hemmschwelle gesehen werden.

Mehr Produktivität mit Password Safe
Was das Tool für Ihre Mitarbeitende bedeutet: Nie wieder ...

... Passwörter auszudenken und merken: Sichere Passwörter (gemäß den internen Passwortrichtlinien) werden auf Knopfdruck erstellt.

... Passwörtern suchen und verlegen: Alle Anmeldedaten werden sicher und übersichtlich in Password Safe gespeichert und verwaltet.

... fehlgeschlagene Logins oder falsch eingegebene Passwörter: Die richtigen Anmeldedaten werden automatisch übertragen.

... Passwörter auf Papier an Kollegen weitergeben müssen: Passwörter werden den entsprechenden Benutzern bereits automatisch zur Verfügung gestellt oder können einfach zugewiesen werden.

... Passwörter manuell zurücksetzen und austauschen: Mit automatischen Passwort Resets in Password Safe und in der Anwendung selbst.

Wie machen wir das?

Training, Training, Training

Anstatt Mitarbeitende zu maßregeln, wenn sie einen Fehler gemacht haben, kann Ihr Unternehmen eine positive Passwortkultur entwickeln, die auch langfristig Bestand hat. Dazu gehört es, für Mitarbeitende eine angenehme Arbeitsatmosphäre zu schaffen, an ihre Teamfähigkeit zu appellieren und sie darin zu fördern, sich als wichtigen Teil des Unternehmens zu betrachten. Denn nur so wird es ihnen bei einem selbst verursachten Fehler leichter fallen, sich anzuvertrauen und zu kooperieren, ohne diesen aus Sorge vor möglichen Konsequenzen gleich unter den Teppich zu kehren.

Ist es aber sinnvoll, alle Mitarbeitenden pro Quartal in einem Raum zu versammeln und ein paar Stunden lang über Sicherheitsfragen zu diskutieren? Es kann nicht schaden, aber es reicht auch definitiv nicht aus. Die eigentliche Praxis, das Gelernte nun auch anzuwenden, findet nämlich vor seinem Schreibtisch im Arbeitsalltag statt. Das ist der Moment, in dem das Wissen in der Praxis angewendet wird. Und zwar meistens dann, wenn niemand zur Verfügung steht, der Hilfestellung gibt oder ein Auge auf das Sicherheitsverhalten hat. **Training bedeutet also nicht einen bestimmten Termin, an dem die Mitarbeitenden erscheinen müssen.** Training findet jeden Tag und jedes Mal statt, wenn der Mitarbeitende mit sicherheitskritischen Prozessen in Berührung kommt. Wie kann man das also lösen?

Fragen Sie sich:

„Sehen Ihre Mitarbeitenden Schulungen nur als Pflichtveranstaltung an oder nehmen sie gerne und vielleicht sogar freiwillig aus eigenem Interesse teil?“

Probleme richtig angehen

Ist es wirklich die Schuld Ihres Social Media Managers, dass er nach 2 Monaten nicht all seine Passwörter geändert hat, oder sollte das vielleicht die Aufgabe der IT-Abteilung sein? Ist diese Anforderung überhaupt etwas, was Ihre Mitarbeitenden selbst umsetzen können, oder sollte das vielleicht ein Tool für sie lösen? Ist es wirklich ihre Schuld, dass etwas nicht funktioniert, oder ist es vielleicht die Schuld des Managements, das viel zu lange weggeschaut hat? Dies sind manchmal Fragen für ein Unternehmen, die wehtun können und sie deshalb nur umso wichtiger machen. Da mehrere Organisationen wie das National Institute of Standards and Technology (NIST) das Problem bereits erkannt und richtig eingeordnet haben, empfehlen sie dringend die Nutzung von Password Managern, um Mitarbeitende bei der Passwort-Problematik zu unterstützen und sie mit den Anforderungen nicht allein zu lassen.

So einfach es auch klingen mag:

Sie wollen, dass Ihre Mitarbeitenden arbeiten? Geben Sie ihnen einen Arbeitsplatz. Sie wollen, dass Ihre Mitarbeitenden nur sichere Passwörter verwenden? Geben Sie ihnen einen Password Manager.

Power-User als Brücke zwischen Technik und Mensch

Sie brauchen Sicherheitspersonal mit einer Open-Door-Philosophie und einem entsprechenden Mindset. Dieses Sicherheitspersonal muss also nicht nur die IT verstehen, sondern auch den Menschen vor dem PC, um eine vertrauensvolle Beziehung aufzubauen und richtig auf ihn eingehen zu können. Nur so kommen die Mitarbeitenden ins Gespräch, kommunizieren transparent und kooperieren, um die bestmögliche Lösung zu finden.

Um dies zu erreichen, können Mitarbeitende außerhalb der IT – z. B. eine Person aus dem Vertrieb, eine aus der Finanzabteilung und eine aus dem Marketing – als Security Promoter ausgewählt werden. Sie sollten auch als Power User für die entsprechenden Tools wie Password Safe geschult werden, damit sie ihren Kollegen richtig helfen können. Diese Security Promoter erhalten nicht nur spezielles Training, sondern kommunizieren auch eng mit ihren Teams, um eine positive Einstellung zu Passwörtern im Unternehmen zu verbreiten und ein Vorbild in Bezug auf die richtige Passworthygiene zu sein. Dieser Power User unterstützt seine Kollegen Tag für Tag, ist immer zur Stelle, wenn eine Frage auftaucht und bietet bei Bedarf Hilfe an.

Power User Skills:

- Führungs-, Erklärungs- und Kommunikationskompetenz
- technische Affinität
- gut vernetzt sein und ein gutes Standing im Team haben
- andere auch für komplexe Themen begeistern können

Zum Beispiel kann ein Mitarbeitender zu ihm kommen, um zu erfahren, wie man ein Passwort sicher mit einem Kollegen teilt oder wie man Zugangsdaten gemeinsam mit einer externen Agentur nutzt. Der Power User zeigt ihm nicht nur die Umsetzung in Password Safe, sondern lässt ihn auch selbst üben, während er weiterhin zur Stelle ist. So kann allein durch die Anwesenheit die Berührungsangst mit neuen Tools und Prozessen abgebaut werden und die Mitarbeitenden werden sicherer im Umgang damit, wodurch wiederum auch die Fehlerhäufigkeit sinkt.

Training ist keine Einbahnstraße

Power User geben ihr Wissen nicht nur weiter, sondern können im Gegenzug auch wichtige Erkenntnisse über die Hürden, Probleme und Bedürfnisse der Mitarbeitenden gewinnen, die der IT-Abteilung selbst vielleicht noch gar nicht bewusst waren. Es ist also eine Win-Win-Situation für das gesamte Unternehmen und Tools und Prozesse können noch besser aufeinander abgestimmt werden. Und das ist noch nicht alles: Mit einem festen Ansprechpartner in Ihrem Team anstelle einer einmaligen Schulung für jeden Mitarbeitenden werden diese eher das Gefühl bekommen, dass eine positive Passwortkultur eine Teamleistung ist, zu der jeder direkt beiträgt.

„Kann ich meinen Sicherheitsbeauftragten jetzt damit belästigen? Vielleicht steht es irgendwo geschrieben und ich habe es übersehen oder hätte es schon längst wissen müssen … Soll ich eine E-Mail schreiben, lieber im Chat schreiben oder wäre es ok, schnell anzurufen?“

Haben Sie die richtigen Kommunikationskanäle?

Wenn nicht wirklich klar ist, wie man jemanden auf welche Weise ansprechen soll, werden die Mitarbeitenden unsicher und ziehen es vor, ihr Problem für sich zu behalten und zu versuchen, es auf eigene Faust zu „lösen“. Dieses unsichere Verhalten kann eine große Gefahr für Unternehmen darstellen. Gerade in Zeiten des ortsunabhängigen Arbeitens ist es wichtig, direkte Kommunikationskanäle zu haben, an die sich Mitarbeitende leicht wenden können, wenn sie Rat und Hilfe benötigen.

Sicherheitsverantwortliche können zum Beispiel einen eigenen Kanal für Passwortprobleme im Team einrichten, in dem rund um die Uhr gepostet werden kann, und kurze Dailies führen, an denen jeder teilnehmen kann, wenn er ein akutes Problem hat. Wie auch immer Ihr Team direkte Kommunikationskanäle einrichten wird: Wichtig ist, dass es ihnen klar und transparent kommuniziert wird.

Glauben Sie an Ihr Team (und zeigen Sie es)

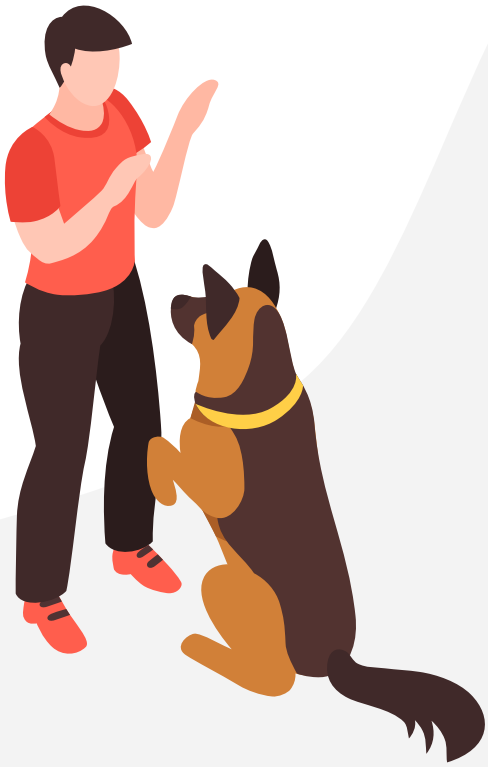
Was ist das Gegenteil von Angst? Es ist Vertrauen – Vertrauen in die eigenen Fähigkeiten, Vertrauen, dass der Mitarbeitende es schaffen wird und dass man an ihn glaubt. Aber wie kann man ihnen das zeigen, wenn es um ein so gefährliches Thema geht, das einen Sicherheitsvorfall verursachen könnte? Indem Sie ihnen einen sicheren Raum bieten, um das Thema selbst anzugehen, und sie dabei aktiv unterstützen.

Um sie selbst üben zu lassen, können Sie zunächst Passwortrichtlinien erst einmal in der Theorie einführen. Mit der Option, Passwörter anhand der in Password Safe implementierten Richtlinien zu überprüfen, kann der Benutzer zunächst selbst ausprobieren, ob er verstanden hat, woraus ein sicheres Passwort bestehen sollte.

Und auch Belohnungen sind ein sicheres Mittel hin zu einer positiven Sicherheitskultur: Zum Beispiel wird der Mitarbeitende mit der stärksten Passwortqualität in den letzten Monaten zum „Passwort-Profi“ in Ihrem Unternehmen – vielleicht sogar mit der Möglichkeit, zum Power User aufzusteigen. So schaffen Sie positive Erfahrungen und motivieren Mitarbeitende, diese auch zu wiederholen und noch besser zu werden. Das stärkt ihr Selbstvertrauen und ihre Fähigkeiten, so dass sie weniger Fehler machen und eine positive Mentalität zu Passwörtern im gesamten Unternehmen verbreiten!

Password Management auf Pawlowisch

Manchen mag der Pawlowsche Hund etwas sagen: Er geht auf das bekannte empirische Experiment des russischen Forschers Iwan Petrowitsch Pawlow zurück, der damit den Nachweis der klassischen Konditionierung erbrachte. Nach der klassischen Konditionierung kann einer natürlichen, meist angeborenen, sogenannten unbedingten Reaktion durch Lernen eine neue, bedingte Reaktion hinzugefügt werden. Bei Pawlows Hund bedeutete dies, dass er beim Ertönen einer Glocke Futter bekam. Nach mehreren Durchläufen reagierte der Hund allein durch den Glockenton mit vermehrtem Speichelfluss.



Auf dieser Grundlage schlug der Sicherheitsexperte Lance James das Pawlowsche Password Management vor. Damit sollen Nutzer langfristig darauf trainiert werden, möglichst sichere Passwörter zu wählen. Bei einem schwachen Passwort wie „test123@#“, das nach 4 bis 5 Tagen geknackt werden kann, würde der Benutzer also aufgefordert werden, es bereits nach 3 Tagen zu ändern. Bei einem komplexeren Passwort hätte der Benutzer 3 Wochen Zeit und bei einer Paraphrase würde er sogar mit einer Zeitspanne von 90 Tagen belohnt werden. Mit dieser Methode sollen die Benutzer darauf konditioniert werden, immer komplexere Passwörter zu verwenden. Diese Methode kann für verschiedene Belohnungsmechanismen adaptiert werden.

Menschliches Versagen oder einfach nur menschlich?

Da sich eine negative Passwortkultur nur darauf bezieht, was man NICHT tun sollte, konzentriert sie sich mehr auf Verbote und mögliche Konsequenzen als auf Chancen und Ursachenforschung. Demgegenüber bietet eine positive Passwortkultur immer eine Lösung für das ursprüngliche Problem: So wird der Mitarbeitende nicht nur als „Human Error“ gesehen, den es zu vermeiden und so gut wie möglich auszuschalten gilt. Er wird als „Mensch“ mit seinen Bedürfnissen, Stärken und Schwächen in den Fokus gesetzt.

So kann das Unternehmen ein Sicherheitskonzept entwickeln, das ihn am besten miteinbezieht und so Sicherheitslücken so lange wie möglich schliesst. Das bedeutet, das Vertrauen jedes einzelnen Mitarbeitenden zu fördern und Sicherheit nicht schwer verständlich zu machen, sondern einfach und sogar mit Spaß individuell umzusetzen. Und damit nicht genug: Eine positive Sicherheitskultur, die auch auf Kommunikation setzt, erhöht die Chance, dass Angestellte der IT mitteilen werden, wenn etwas bereits schief gelaufen ist oder in Zukunft schief laufen könnte. So kann der potenzielle Schaden so gering wie möglich gehalten werden.

„Human Error“, „DAU“ oder „Layer8“ waren gestern

Machen Sie die Mitarbeitende nicht zum Teil des Problems, sondern zum Teil Ihrer Lösungen!

Exkursion: Wo eine positive Passwort-Kultur am besten gedeiht

Die Arbeit von zu Hause aus ist zur neuen Normalität geworden – spätestens seitdem Corona uns im Jahr 2020 sehr schnell dazu gezwungen hat. Aber sind die Arbeitnehmer damit zufrieden? Offenbar und laut Studien schon. Einige Unternehmen befürchteten anfangs, dass die Produktivität bei der Arbeit von zu Hause aus nachlassen könnte. Doch sie lagen meist falsch, denn die Mitarbeitenden wollten ihrer neu gewonnenen Freiheit, zu Hause zu arbeiten, gerecht werden und sie unter keinen Umständen aufs Spiel setzen. Außerdem konnten sie nun ungestörter, entspannter und mit weniger Ablenkungen (besser) arbeiten. Das bedeutet aber auch, dass sie für den Arbeitgeber weniger sichtbar sind, da sie in ihrem eigenen Heimnetzwerk oder vielleicht sogar in einem offenen Netzwerk in einem Café in der Nähe arbeiten ...

Brauchen Sie also Ihre Angestellten im Büro, um mehr Sicherheitsbewusstsein zu schaffen? Sicherlich nicht: Das Vertrauen, das in Mitarbeitende gesetzt wird, die von zu Hause aus arbeiten, verstärkt den Glauben, dass ihr bisheriges Passwortverhalten geschätzt und belohnt wird. Und eine vertrauensvolle Beziehung, in der Cybersicherheit als positiv und motivierend erlebt wird – kombiniert mit den richtigen Tools und Sicherheitsvorkehrungen wie VPN und einem Password Manager – kann von überall aus funktionieren!

Zusammenfassung: Immer positiv bleiben

Negative Passwort-Kultur	Positive Passwort-Kultur
• nur kurzfristige Ziele und Erfolge	• langfristige Ziele und Erfolge
• extrinsische Motivation: kein Einfluss auf höhere Priorisierung von Sicherheit	• intrinsische Motivation: Mitarbeitende „leben“ und verinnerlichen die Methoden
• Sicherheit = Stopper: Mitarbeitende vermeiden / ignorieren Sicherheitsstandards aus Unverständnis heraus	• Sicherheit = Befähiger: Mitarbeitende sehen den eigenen positiven Nutzen für ihre Arbeit
• Erschwerung der Sicherheit, da Angst das Denken blockiert	• Sicherheit wird leichter anwendbar und nutzbar für alle gemacht
• Maßnahmen: einseitige Schulungen, zu wenig Austausch, Maßregelungen und Androhung von Konsequenzen	• Maßnahmen: direkte Ansprechpartner, um Probleme zu lösen, Mitarbeitende täglich zu trainieren und und sicherheitsrelevante Entscheidungen zu belohnen
• behindert die Produktivität, da rationale Entscheidungen blockiert werden	• steigert die Produktivität, da der eigene Nutzen erkannt und angewendet wird
• negative Atmosphäre provoziert Nähe zu mehr (vermeidbaren) Fehlern	• zahlt auf ein positives Arbeitsklima ein, das auch für weniger Fehler sorgt

Tipps zum Schluss: Positive Passwort-Kultur verbreiten

- **Leben Sie es vor:** Ihre Angestellten brauchen Vorbilder, die ihnen den Weg weisen. Integrieren Sie z.B. Password Safe Power User / Evangelisten, die als direkte Ansprechpartner im Unternehmen fungieren, wenn Fragen auftauchen oder Mitarbeitende Anleitung benötigen.
- **Setzen Sie die Theorie in die Praxis um:** Haben Ihre Mitarbeitenden die richtigen Werkzeuge, um die Sicherheitsvorkehrungen in die Praxis umzusetzen? Stellen Sie sicher, dass die Nutzung so einfach wie möglich ist, und bieten Sie Einführungen, Tutorials und Hilfe bei der Nutzung neuer Tools an.
- **Schaffen Sie eine positive Erfahrung:** Ihre Angestellten haben ihr Passwort vergessen? Sie wissen nicht, wie sie es mit den Teammitgliedern teilen können? Stellen Sie sicher, dass Sie ihnen wirklich zuhören, sie ernst nehmen und ihnen sichere Lösungen für ihre Probleme anbieten.
- **Belohnen Sie passwortbewusstes Verhalten:** Loben Sie Teammitglieder, die Sicherheitsprobleme ansprechen, Hilfe benötigen oder ihre Erfahrungen mit Passwörtern weitergeben, damit sie in Zukunft eher bereit sind, ihre Probleme zu teilen. So können auch andere davon lernen und fühlen sich mit ihren Problemen weniger alleine.

Autor:
Kristina Kaya
Product Marketing Managerin

MATESO
PASSWORD SAFE

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 21 Firmen der Dax 40.

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.

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

MATESO
PASSWORD SAFE