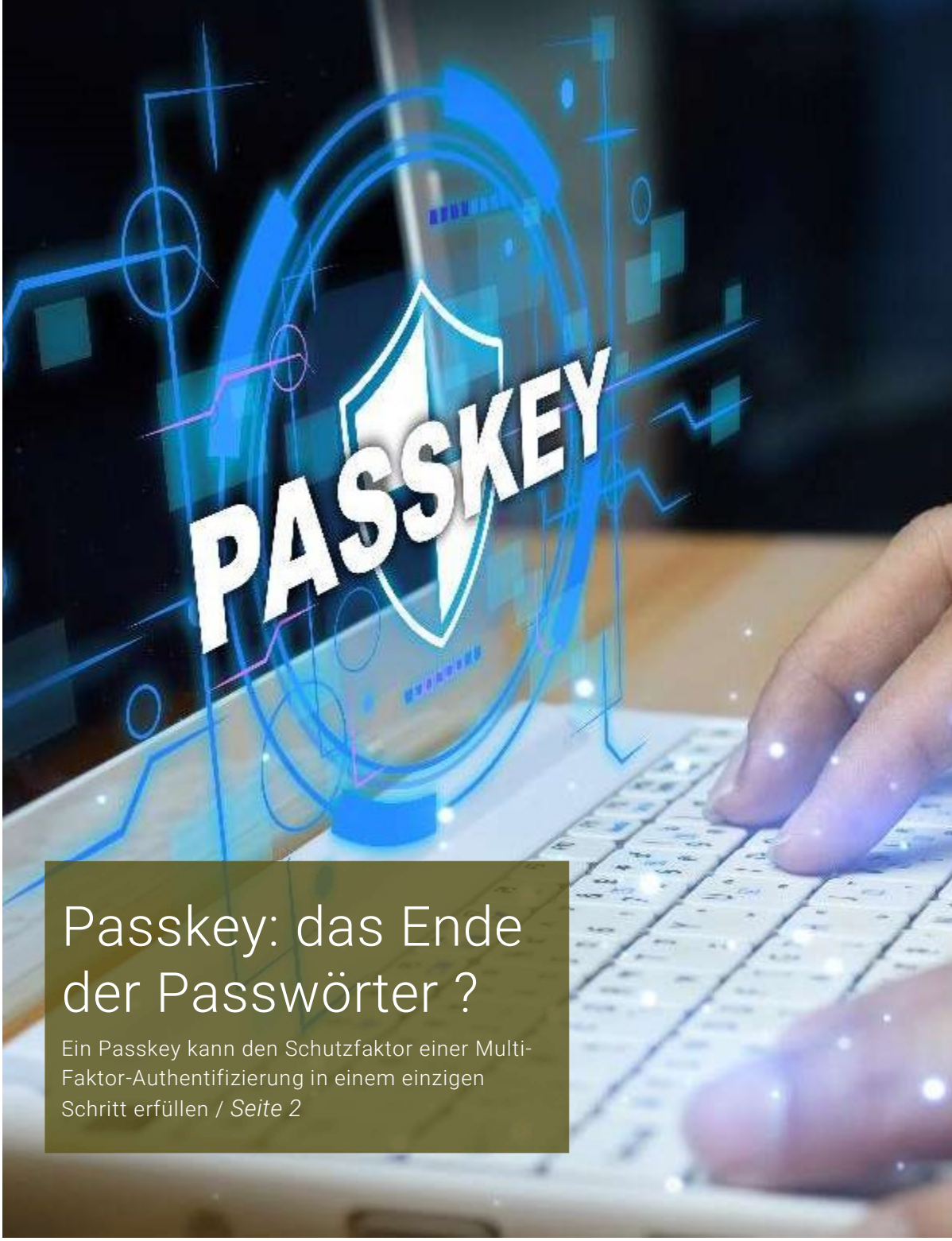
Datenschutz Radar

Eine Ausgabe von DSBOK.de | April 2025



Passkey: das Ende der Passwörter ?

Ein Passkey kann den Schutzfaktor einer Multi-Faktor-Authentifizierung in einem einzigen Schritt erfüllen / *Seite 2*

INHALT:

Liebe Leserin, lieber Leser,

wenn man sich gut kennt, steigt das Vertrauen. Was im zwischenmenschlichen Bereich positiv ist, kann im Datenschutz schnell zu einem Risiko werden. So ist zum Beispiel das Thema der **sicheren Passwörter** ein wahres Evergreen im Datenschutz. Das bedeutet aber nicht, dass man dem Passwortschutz wirklich vertrauen kann. Erfahren Sie im ersten Beitrag, wie es wirklich um die Passwortsicherheit steht und was sich hier ändern könnte.
Auch das Excel-Programm ist ein alter Bekannter. Doch man kann damit nicht nur Tabellenkalkulation machen, mit **Excel-Dateien** können auch Datenpannen verbunden sein, wie der zweite Beitrag zeigt. Die Gefahr durch **Social Engineering** scheint ebenfalls inzwischen bekannt zu sein.

Doch wissen Sie, wie Sie dieser Gefahr richtig begegnen können? Der dritte Beitrag verrät es.
Die neue Ausgabe schließt mit einer weiteren Überraschung: **Schadprogramme** fängt man sich nicht nur im Internet ein. Erfahren Sie, was Ihnen bei der ersten **Nutzung eines Neuprodukts** bereits drohen kann. Die IT-Sicherheitsbehörde BSI hat von einer konkreten Gefahr berichtet. ■

Oliver Krause
Externer Datenschutzbeauftragter
Datenschutzauditor
ok@dsbok.de

■ Kommt das Ende der Passwörter?

Die Forderung nach sicheren Passwörtern besteht seit vielen Jahren, und jedes Jahr findet ein „Change Your Password Day" statt, um an einen notwendigen Wechsel der Passwörter zu erinnern. Doch wie steht es um die Passwortsicherheit, und was sind Passkeys, die Passwörter ersetzen könnten?

Passwörter sind ein doppelter Klassiker, im Zugangsschutz und als Risiko

So mancher kann es kaum noch hören: „Denken Sie daran, sichere Passwörter zu wählen!" Trotz der fortlaufenden Sicherheitshinweise bleibt die Passwortsicherheit aber eine Herausforderung. Laut Umfrage des Digitalverbands Bitkom nutzt rund ein Viertel (23 Prozent) der Internetnutzerinnen und -nutzer häufig bewusst einfache Passwörter, damit sie sich diese leicht merken können. Ein Drittel (33 Prozent) nutzt dasselbe Passwort für verschiedene Dienste.

Das empfehlen Security-Expertinnen und -Experten

Passkeys können auf Phishing-Webseiten nicht funktionieren, denn sie sind immer nur mit einer definierten Website oder App verknüpft.

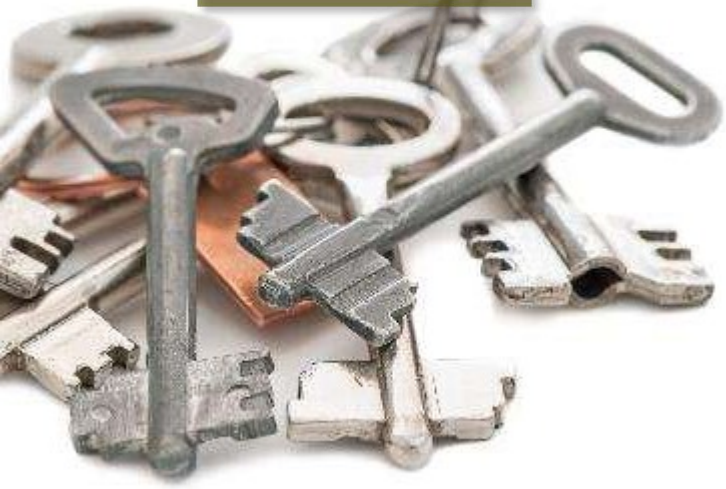
Bereits diese Erhebung macht deutlich: Die Empfehlungen zur Wahl sicherer Passwörter werden oft genannt, sie stoßen aber auf taube Ohren. Das ist für den Datenschutz sehr riskant, denn Passwörter werden als Zugangsschutz in vielen sensiblen Bereichen genutzt, zum Beispiel für E-Mail- und Unternehmens-kommunikation, soziale Netzwerke oder Cloud-Speicher.

Passwörter müssen selbst geschützt werden

Auch wenn Passwörter weiterhin häufig als Mittel der Wahl im Schutz vor unerlaubten Zugriffen auf Nutzerkonten gelten, benötigen sie selbst einen zusätzlichen Schutz. Da viele Nutzerinnen und Nutzer zu einfachen und immer gleichen Passwörtern neigen, kommt es auf eine weitere Schutzschicht an. Moderne Passwort-Manager und Zwei-Faktor-Authentifizierung (2FA) reduzieren die Notwendigkeit ständiger Passwortwechsel und erleichtern die sichere Verwaltung digitaler Zugangsdaten, so empfehlen Security-Expertinnen und -Experten.

Passwort Manager ?

Moderne Passwort-Manager und Zwei-Faktor-Authentifizierung (2FA) reduzieren die Notwendigkeit ständiger Passwortwechsel, aber…



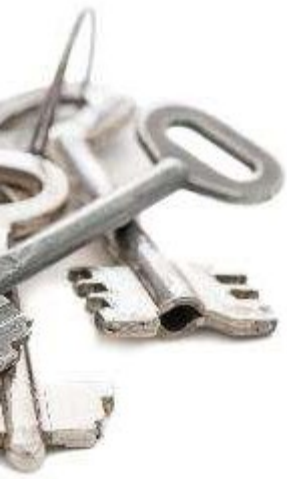
Passwort-Manager zum Beispiel generieren komplexe, einzigartige Passwörter für jede Anwendung und speichern sie verschlüsselt. Dies hilft insbesondere Personen, die aus Gewohnheit ein Passwort für mehrere Konten verwenden. Zwei-Faktor-Authentifizierung (2FA) erschwert den Zugriff für unbefugte Dritte, selbst wenn ein Passwort kompromittiert wurde, da zum Beispiel zusätzlich der Fingerabdruck überprüft wird.

Passkeys können Passwörter ersetzen

Einfache Nutzernamen-Passwort-Kombinationen sind unsicher, Zwei-Faktor-Authentifizierung empfinden aber viele Nutzerinnen und Nutzer als umständlich. Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) bieten Passkeys ein deutlich höheres Sicherheitsniveau als herkömmliche Verfahren.

Passkeys sind eine neue Möglichkeit, sich bei Apps und Websites anzumelden. Anstelle von Benutzername und Passwort können sich Benutzer mit Passkeys bei Apps und Websites auf dieselbe Weise anmelden, wie sie ihre Geräte entsperren: mit einem Fingerabdruck, einem Gesichtsscan oder einer PIN für die Bildschirmsperre.

Passkeys bestehen aus einem öffentlichen und einem privaten Schlüssel, um die sich die Nutzerin oder der Nutzer aber nicht kümmern muss. Geschützt wird der private Schlüssel meist über Fingerabdruck oder Gesichtsscan.



Ein Passkey kann so den Schutzfaktor einer Multi-Faktor-Authentifizierung in einem einzigen Schritt erfüllen. Anwenderinnen und Anwender können bei Passkeys ihre Zugangsinformationen nicht mehr versehentlich weitergeben, denn sie haben diese nicht im Zugriff. Selbst wenn Passkeys anderweitig genutzt würden: Passkeys können auf Phishing-Webseiten nicht funktionieren, denn sie sind immer nur mit einer definierten Website oder App verknüpft. Passkeys könnten das Ende der Passwörter einläuten, doch noch ist es nicht so weit, noch sind sie zu unbekannt.

Tipps für sichere Passwörter

Da Passkeys noch nicht so verbreitet sind, bleiben die Sicherheitshinweise zur Wahl besserer Passwörter wichtig. Es gilt also weiterhin: Passwörter sollten nicht aus einem leicht zu erratenden Begriff oder aus einem im Wörterbuch zu findendem einzelnem Wort bestehen. Für jeden Online-Dienst und jeden einzelnen Zugang sollte man ein einzigartiges Passwort verwenden. Passwörter auf Notizzettel und in Textdateien sind eine Gefahr, eine sichere Aufbewahrung ist in einem Passwort-Manager möglich. Wo immer möglich, sollte die Zwei-Faktor-Authentifizierung (2FA) eingerichtet werden. ■

Passen Sie auf

Beim Öffnen ist zunächst nur das erste Arbeitsblatt sichtbar. Weitere Arbeits-blätter, die ebenfalls Daten enthalten, sind dann schnell übersehen oder vergessen.

Wird die Excel-Mappe weitergegeben, werden sie mit übermittelt. Wenn das nicht erforderlich war und personenbezogene Daten enthalten sind, stehen wir vor einer Datenpanne.

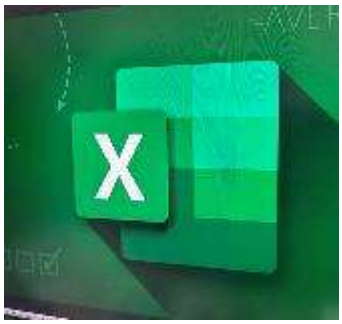
■ Datenpannen bei Excel vermeiden!

Excel ist ein gutes und wichtiges Werkzeug für den Büroalltag. Wer es ungeschickt benutzt, kann damit aber auch sehr schnell Datenpannen verursachen. Das ließe sich meist leicht vermeiden. Achten Sie deshalb auf typische Fallstricke!

So schnell geschieht eine Panne

Morgen früh braucht ein Dienstleister die Liste mit Namen und Anschrift bestimmter Kundinnen und Kunden, an die er im Auftrag Ihres Unternehmens einen

Sonderkatalog verschicken soll. Sie ziehen die nötigen Daten aus einer Excel-Tabelle heraus, in der alle Kundinnen und Kunden enthalten sind. Sie speichern die Daten in einem eigenen Arbeitsblatt, aber in einer Arbeitsmappe zusammen mit anderen Arbeitsblättern, die von früheren ähnlichen Aktionen stammen. Dann schließen Sie die Arbeitsmappe, weil Sie etwas anderes erledigen müssen.



Am nächsten Morgen sind Sie nicht da. Ihre Vertretung übernimmt die Weiterleitung an den Dienstleister. Dabei übersieht sie, dass die Excel-Datei mehrere Arbeitsblätter mit Daten enthält. Das Ergebnis: Der Dienstleister bekommt Daten, die er weder will noch braucht.

Das war der Fallstrick

Abstrakt ist es wohl allen klar: Eine Excel-Arbeitsmappe kann – solange der Arbeitsspeicher ausreicht – beliebig viele Arbeitsblätter enthalten. Beim Öffnen ist jedoch zunächst nur das erste Arbeitsblatt sichtbar. Weitere Arbeitsblätter, die ebenfalls Daten enthalten, sind dann schnell übersehen oder vergessen. Wird die Excel-Mappe weitergegeben, werden sie mit übermittelt. Wenn das nicht erforderlich war und personenbezogene Daten enthalten sind, stehen wir vor einer Datenpanne. Sie kann nach den Vorgaben der DSGVO meldepflichtig sein.

Manchmal ist Excel schlicht entbehrlich

Excel ist ein Tabellenprogramm. Seine Stärken kann es dann ausspielen, wenn die Arbeit mit Tabellen Vorteile in der Sache bringt. Selbstverständlich kann man es aber auch für die Erstellung von Texten und dergleichen nutzen. Dafür würde aber auch jedes Textverarbeitungsprogramm reichen. Dann sollte man Excel besser außen vorlassen. Denn auch im Büro gilt: Bei jeder Arbeit sollte man das Werkzeug benutzen, das dafür gedacht und dafür am besten geeignet ist.

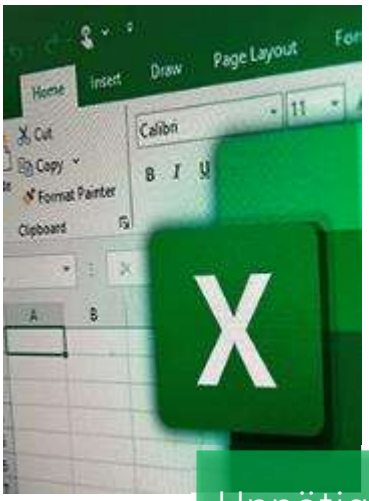
Eine Arbeitsmappe sollten Sie sinnvoll strukturieren

Arbeitsmappen, die mehrere oder vielleicht sogar viele Arbeitsblätter enthalten, fördern Datenpannen. Dies hat das Eingangsbeispiel deutlich gezeigt. Wenn Sie eine Arbeitsmappe neu anlegen, sollten Sie daher bewusst überlegen, wie viele Arbeitsblätter Sie darin voraussichtlich brauchen. Oft werden ein oder zwei Arbeitsblätter ausreichen. Dann sollten Sie die Zahl der Arbeitsblätter auch entsprechend begrenzen.

Unnötige Arbeitsblätter sollten Sie löschen

Wenn Sie noch nicht wissen, wie viele Arbeitsblätter nötig sind, können Sie ruhig mit einer größeren Zahl von Arbeitsblättern starten. Sobald die Arbeit abgeschlossen ist,

sollten Sie nicht mehr benötigte Arbeitsblätter aber konsequent löschen. Wenn Sie sich das als Routine angewöhnt haben, kostet es kaum Zeit, beugt Datenpannen aber sehr effektiv vor.



Ein PDF kann von Vorteil sein

Wer eine Excel-Datei von einer anderen Person erhält, kann in der Datei sofort weiterarbeiten. Das ist in vielen Situationen von großem Vorteil. Oft genug wollen Empfängerinnen und Empfänger von Daten jedoch nur sehen, was inhaltlich in der Datei steht. Dann reicht es völlig aus, ihnen eine PDF-Version zu übermitteln. Eine PDF-Version lässt sich vor dem Versand mit wenigen Blicken auf versteckte Daten kontrollieren.

Unnötige Arbeitsblätter sollten Sie löschen.

Sobald die Arbeit abgeschlossen ist, sollten Sie nicht mehr benötigte Arbeitsblätter aber konsequent löschen.

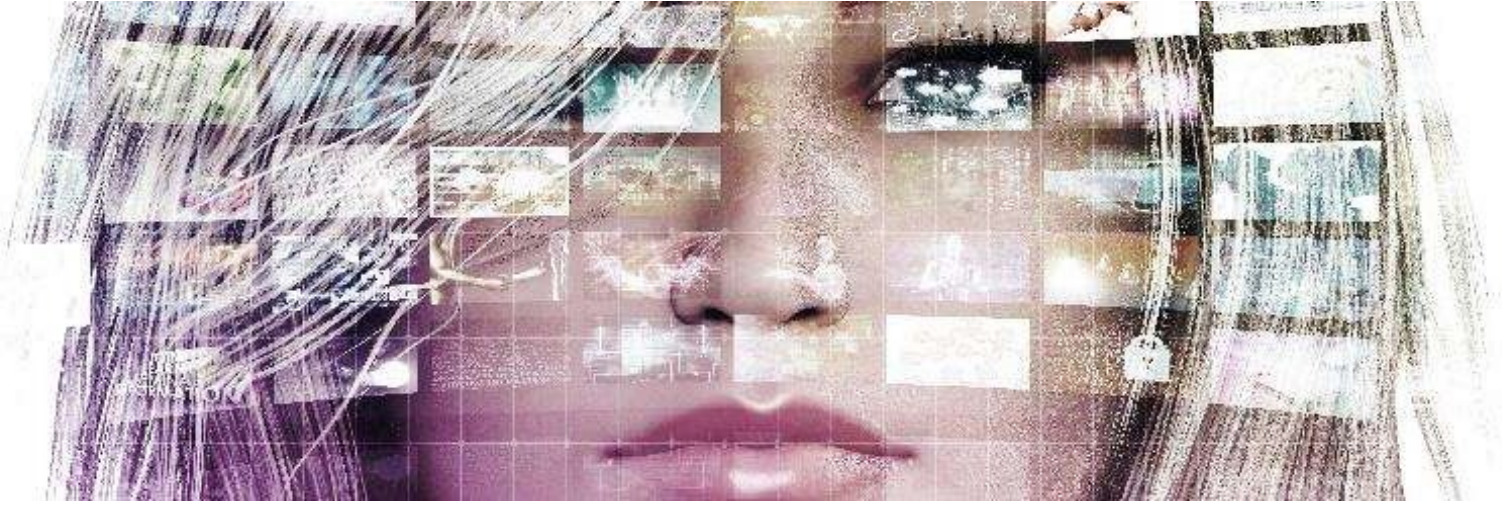
Die unsichtbaren Daten sind das Tückische

Zu Daten, die in einzelnen Feldern enthalten sind, können zusätzliche Informationen hinterlegt sein. Oft sind sie personenbezogen. Hierzu ein Beispiel: Im Menü „Überprüfen“ gibt es den Punkt „Änderungen nachverfolgen – Änderungen hervorheben“. Dahinter steckt eine Funktion, mit der Sie für die entsprechend ausgewählten Zellen die Protokollierung von Änderungen vorsehen können.

Aus dieser Protokollierung ist zu entnehmen, wer eine Änderung vorgenommen hat und wann. Die entsprechenden Zellen erhalten zwar eine Markierung, wenn man bei ihnen diese Funktion nutzt. Die Protokollierungsinformationen selbst sind aber nur zu sehen, wenn die betreffende Zelle gerade aktiv ist oder der Mauszeiger darüberstreicht.

Nutzen Sie Schulungsangebote!

Je besser Sie Excel beherrschen, desto eher können Sie Datenpannen vermeiden. Abgesehen davon ist es auch sonst von Vorteil, sich mit diesem Programm möglichst gut auszukennen. Denn dann geht vieles im Büroalltag besser von der Hand. Excel an sich ist bezüglich des Datenschutzes in Ordnung – vorausgesetzt natürlich, dass Sie es sachkundig einsetzen! ■



Der „Kollege“ ist nicht echt – aber Sie als Opfer schon!

Kriminelle geben sich als jemand aus, der sie in Wirklichkeit gar nicht sind. So bringen sie das Opfer dazu, vertrauliche Informationen preiszugeben. Und schon haben Sie als Opfer ein Datenschutzproblem. Das steckt hinter dem Begriff „Social Engineering“. Schützen Sie sich davor!

Nehmen Sie Schulungen ernst!

Es hat seine guten Gründe, sollte das Unternehmen Schulungen anbieten, um für die Gefahren von Social Engineering zu sensibilisieren. Nutzen Sie solche Angebote und denken Sie über die Beispiele wirklich nach! Auch über die Beispiele, die auf den ersten Blick eher kurios wirken....

Das könnte auch Ihnen passieren

Die meisten Menschen glauben, dass ihnen Manipulationen auffallen würden. Die Fakten sprechen aber eine andere Sprache. Einen sprichwörtlichen „schlechten Tag“ haben wir alle einmal. Der Kopf tut weh, ein Kunde stresst, die Kollegin oder der Kollege ist aus irgendeinem Grund sauer. Dann klingelt das Telefon. Ein Anrufer, angeblich neuer Mitarbeiter in der IT-Abteilung, macht Druck. Er will von Ihnen ein Passwort für ein sofort notwendiges Update. Dabei lässt er anklingen, dass Sie etwas grob falsch gemacht hätten am PC. Das sind Situationen, in denen es schnell passiert ist: Der Kriminelle am anderen Ende der Leitung hat Erfolg und Sie geben das Passwort heraus.

Attacken können unspektakulär wirken

Über das Beispiel eben lächeln Sie vielleicht. Sie sind sicher, dass Ihnen das ganz bestimmt nicht passieren würde. Das mag tatsächlich so sein. Aber wie sähe es aus, wenn der Anrufer nicht nach einem Passwort fragt? Sondern „nur“ ein paar Angaben über die Software möchte, die Sie benutzen. Seine nebenbei hingesagte Begründung dafür lautet, die Unterlagen in der IT seien unvollständig, Schlampereien seines Vorgängers halt. Und jetzt solle alles besser werden.

Jetzt würden Sie vielleicht doch antworten. Vor allem, falls Ihnen Schlampereien in der IT vielleicht glaubwürdig erscheinen. Damit sind wir beim Kernpunkt von „Social

Engineering“: Wir sind alle manipulierbar, lediglich unsere Schwachstellen sind unterschiedlich. Und schon verfügt der Anrufer über eine Information, die er zusammen mit anderen Informationen sehr effektiv für seine kriminellen Zwecke nutzen kann.

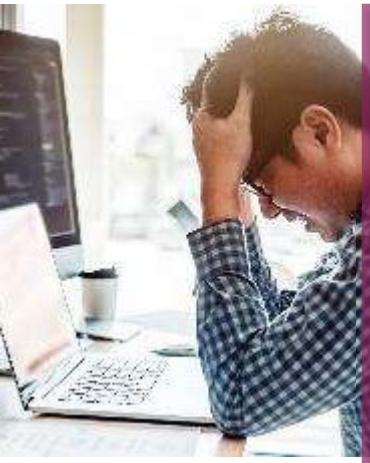
Festgelegte Abläufe haben ihren Sinn

Alle haben es schon erlebt: Was als Ablauf vorgegeben ist, ist eine Sache. Was daraus in der Praxis gemacht wird, ist oft etwas anderes. Halten Sie sich also an das, was vorgegeben ist! Wenn Abläufe für die Weitergabe von Informationen festgelegt sind, schützt ihre Einhaltung auch gegen Manipulationsversuche durch Kriminelle.

Sicherheitsmechanismen sind ein guter Schutz

Sicher ist Ihnen aufgefallen, dass Sicherheitsmechanismen immer ausgefeilter werden. Ein Beispiel hierfür sind Multi-Faktor-Authentifizierungen, bei denen neben dem Passwort zum Beispiel ein Code auf dem Smartphone oder eine Keycard benötigt wird. Nutzen Sie auch in Ihrem privaten Bereich entsprechende Angebote! Dies sollten Sie selbst dann tun, wenn die Einrichtung entsprechender Abläufe zunächst etwas Aufwand erfordert. Dieser Aufwand lohnt sich.

Im Hintergrund geschieht recht viel



Wirklich wichtig sind aber Sie.

Nahezu jedes technische System kann unter bestimmten Bedingungen überwunden oder ausgebremst werden. Dies geschieht durch menschliches Handeln. Das ist gemeint, wenn immer wieder scheinbar geringschätzig davon gesprochen wird, die eigentliche Schwachstelle sei der Mensch.

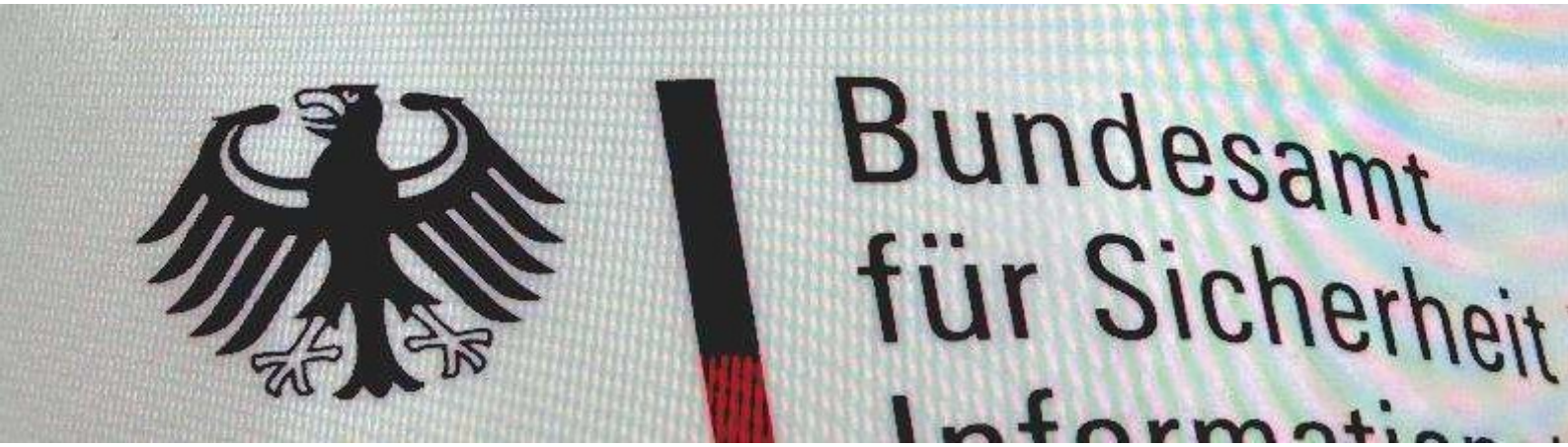
Denkt man genauer darüber nach, folgt daraus jedoch andererseits: Der Mensch – und damit sind Sie gemeint – ist unentbehrlich, wenn es um die Abwehr von kriminellen Attacken geht.

IT-Sicherheitssoftware wie Spam-Filter oder Anti-Phishing-Software erschweren Angriffe, beispielsweise mittels Mails. Auch kommen spezielle softwarebasierte Systeme zum Einsatz, um ungewöhnliche Aktivitäten im Unternehmensnetzwerk zu entdecken. Dies geschieht im Hintergrund, ohne dass darüber groß geredet würde, und das ist auch gut so. Denn genauere Informationen darüber könnten für Kriminelle Gold wert sein. Für Sie wiederum ist es eine Beruhigung, was hier alles veranlasst wird.

Daraus folgen konkrete Bitten an Sie

Seien Sie misstrauisch, wenn etwas „komisch wirkt“. Oft genug stimmt dann tatsächlich etwas nicht. Fragen Sie dann lieber einmal bei der passenden Stelle im Unternehmen nach. Und wenn Sie den Eindruck haben, dass Sie tatsächlich

hereingelegt worden sind, melden Sie es gleich. Oft lässt sich dann ein Schaden noch verhindern oder jedenfalls verringern. ■



■ Schadsoftware ab Werk

IT-Sicherheitsbehörden warnen davor, dass auf IT-Geräten schon vor der ersten Nutzung Schadprogramme installiert sein können. Es reicht also nicht, sich vor Malware aus dem Internet zu schützen. Die Schadsoftware kann bereits auf dem Gerät sein, das sich noch in dem Versandkarton befindet.

Die Firewall ins Internet reicht nicht

Es ist Teil vieler IT-Sicherheits- und Datenschutzschulungen: Man soll nicht ungeprüft einfach auf jeden Link klicken, der per E-Mail oder Chat-Nachricht kommt. Ebenso soll man nicht ohne Weiteres die Dateien im Anhang der Nachricht öffnen.

Auch beim Internetsurfen mit dem Webbrowser ist Vorsicht geboten: Hinter dem Suchtreffer bei einer Suchmaschine kann auch eine mit Schadsoftware verseuchte Website stecken. Dabei reicht es, die Webseite zu öffnen, man muss nichts weiter anklicken. Man spricht dann von dem „Herunterladen im Vorbeifahren“ (Drive-by-Download), also einer Malware-Infektion ohne weiteres Zutun, das Öffnen der Internetseite reicht.

Nun könnte man denken, die Schadprogramme lauern im Internet oder kommen per E-Mail oder Chat aus dem Internet. Ein Schutz mit Firewall und Virenschutz ist deshalb entscheidend. Das stimmt zwar, aber es reicht nicht.

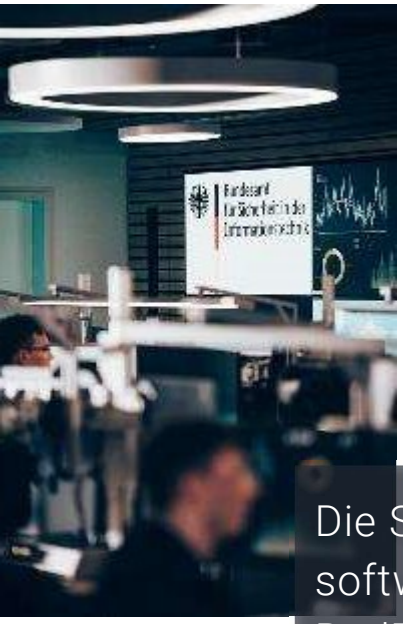
BSI warnt vor verseuchten Geräten

Vor wenigen Monaten warnte die IT-Sicherheitsbehörde BSI (Bundesamt für Sicherheit in der Informationstechnik): Digitale Bilderrahmen oder Mediaplayer, die

Vorinstallierte Malware bei Neuprodukten

Die Warnung des BSI stellt klar, dass nicht erst die Verbindung mit dem Internet eine Prüfung auf Befall mit Malware notwendig macht, sondern bereits der Moment, in dem man das Gerät auspackt und das erste Mal nutzen möchte.

mit dem Internet verbunden werden, können mit Schadsoftware infiziert werden und sind daher immer öfter Ziel von Cyberkriminellen. Das Bundesamt für Sicherheit in der Informationstechnik hat bei bis zu 30.000 solcher Geräte in Deutschland die Kommunikation zwischen der Schadsoftware BadBox und den Tätern unterbunden. All diesen Geräten ist gemein, dass sie über veraltete Android-Versionen verfügen und mit vorinstallierter Schadsoftware ausgeliefert wurden.



BadBox ist in der Lage, unbemerkt Nutzerkonten für E-Mail- und Messenger-Dienste zu erstellen, über die anschließend Fake-News verbreitet werden können, so das BSI. Weiterhin kann BadBox Werbebetrug (Ad-Fraud) durchführen, indem es im Hintergrund Webseiten ansteuert.

Das BSI machte bei diesem Beispielfall deutlich: Hersteller und Händler haben die Verantwortung dafür, dass solche Geräte nicht auf den Markt kommen. Aber auch Nutzende können etwas tun: Schon beim Kauf sollte Cybersicherheit ein wichtiges Kriterium sein.

Die Schad-software BadBox

war in allen dem BSI bekannten Fällen bereits beim Kauf auf den jeweiligen Geräten installiert…

Dabei ist das Risiko durch vorinstallierte Malware bei Neuprodukten nicht auf Mediaplayer, digitale Bilderrahmen oder das Betriebssystem Android beschränkt. Letztlich können alle Arten von Geräten, auf denen sich etwas installieren lässt, betroffen sein.

Vor der ersten Nutzung an Virenprüfung denken

Die Warnung des BSI stellt klar, dass nicht erst die Verbindung mit dem Internet eine Prüfung auf Befall mit Malware notwendig macht, sondern bereits der Moment, in dem man das Gerät auspackt und das erste Mal nutzen möchte.

Das BSI empfiehlt grundsätzlich, vor dem Kauf entsprechender Produkte, die Sicherheitseigenschaften des Geräts zu überprüfen. Empfehlenswert sind ein offizieller Hersteller-Support, eine aktuelle Version des jeweiligen Betriebssystems und ein Blick auf die Seriosität des Herstellers.

Die Cybersicherheit der Geräte

Bisher ist die Cybersicherheit von Geräten kein Teil der Produktsicherheit. Erst Ende 2027 müssen neue, vernetzte Produkte die Anforderungen aus dem sogenannten Cyber Resilience Act (CRA) erfüllen, dann ist die Cybersicherheit ein Teil der Produktsicherheit.

Nicht zuletzt sollte auch eine Prüfung auf Virenbefall stattfinden. Antivirensoftware führt dies in aller Regel bereits während der ersten Installation durch, es muss aber auch eine regelmäßige Aktualisierung der Schutzsoftware stattfinden. ■