Nr. 68/2025

tele-news

TIPPS UND TRENDS FÜR IHRE TELEKOMMUNIKATION

Hösel
Fernmelde- & Computerservice

Mario Hösel
Geschäftsführung
Fernmelde- & Computerservice
Hösel

Liebe Leserin, lieber Leser,

ein einziger Moment kann heute über Erfolg oder Stillstand entscheiden – sei es durch eine Phishing-Mail, ein unsicheres Passwort oder einen Netzwerkausfall. Wer Daten, Systeme und Prozesse absichert, schützt nicht nur sein Unternehmen, er gewinnt Vertrauen und signalisiert Zukunftsfähigkeit. In dieser Ausgabe zeigen wir Ihnen praxisnahe Lösungen: Mit Passwortmanagern und Hardware-Authentifizierung stärken Sie den Zugangsschutz. Ein Router mit Mobilfunk-Backup sichert Ihr Netz gegen Ausfälle und Kaspersky Security Awareness sensibilisiert Ihre Mitarbeitenden – die wichtigste Verteidigungslinie. Gemeinsam mit Ihnen schaffen wir Sicherheit mit System.

Omada DR3220v-4G Router von TP-Link

Keine Panik bei Netzausfall

Foto: freepikcompany

In einer Welt, in der digitale Prozesse den Geschäftserfolg bestimmen, ist die durchgängige Verfügbarkeit des Netzes ein existenzielles Muss. Immer mehr Unternehmen setzen deshalb auf redundante Netzwerklösungen.

Montagmorgen, kurz nach acht: In der Buchhaltung eines mittelständischen Unternehmens herrscht Hochbetrieb. Rechnungen, Monatsabschluss, wichtige Finanzdaten – alles läuft auf Hochtouren. Doch plötzlich steht alles still. Kein Internet, keine Telefonie, keine E-Mails. Auch in der Produktion: Maschinen bereit, Mitarbeitende startklar – doch ohne Netzwerk keine Verbindung zum ERP-System, keine Kommunikation mit Kunden, keine Auftragsdaten. Die Folgen: Produktionsausfall, Lieferverzug, finanzielle Verluste.

Online auch ohne Kabel

Ein Szenario, das erschreckend real ist – aber vermeidbar. Während kabelgebundene Ausfallsicherheit über Kupfer oder Glasfaser oft dieselbe Infrastruktur nutzt und so bei einem Kabelbruch gemeinsam ausfällt, arbeitet das Mobilfunknetz über eine komplett separate Architektur – und bleibt selbst dann funktionsfähig, wenn die Erdleitungen durchtrennt sind.

Ausfallsicherheit für den Geschäftsbetrieb

TP-Link hat mit dem Omada DR3220v-4G Router eine Lösung, die Unternehmen genau für solche Szenarien wappnet. Der Business-Router verfügt über integrierten 4G/LTE-Support und schaltet bei Ausfall des kabelgebundenen Netzes automatisch auf das Mobilfunknetz um. So bleiben Anwendungen, Dienste und Prozesse durchgängig erreichbar. Zudem integriert sich der DR3220v-4G nahtlos in die Cloud-basierte Netzwerkplattform Omada SDN von TP-Link. Diese ermöglicht zentrale Netzwerkverwaltung und Fernwartung. Eine KI-gestützte Analyse erkennt frühzeitig Anomalien im Netzwerk, reagiert automatisch auf Leistungseinbrüche und ermöglicht die proaktive Überwachung via intuitivem Dashboard.

Stabile Konnektivität

Ausfallsicherheit und durchgehende Verfügbarkeit des IT-Netzes sind ein echter Gamechanger für Unternehmen, die auf kontinuierliche Netzwerkkonnektivität angewiesen sind. Mit einem garantierten Service-Level von 99,99 Prozent und geografisch verteilten Backup-Servern bleibt das Omada-Netzwerk auch bei Störungen im zentralen Management verfügbar– ein weiterer Pluspunkt in puncto Ausfallsicherheit. Für Unternehmen, deren Workflow auf durchgängig stabilen Netzverbindungen basiert, ist diese Lösung mehr als nur ein Sicherheitsnetz – sie ist ein echter Wettbewerbsvorteil. ■

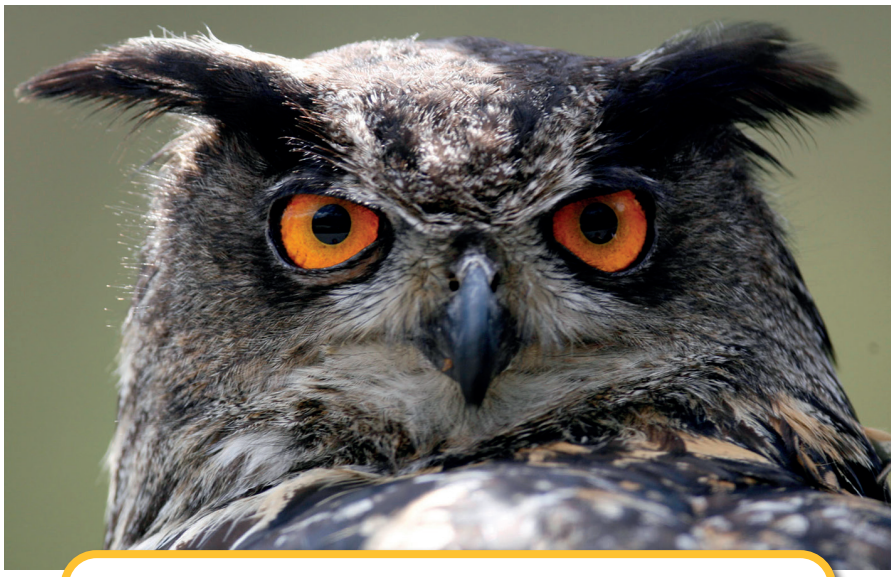
Wenn Sie Fragen zum Thema „Einsatz von moderner Informations- und Kommunikationstechnologie“ haben, wählen Sie diese Telefon-Nummer:

0 37 360 - 69 08 0

Die Mitarbeiter der Firma Fernmelde- & Computerservice Hösel beraten Sie gern!

All-in-One-Lösung für die Zugriffsverwaltung

Keeper – mehr als nur sichere Passwörter

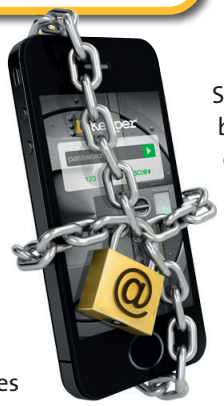


Ein Passwortmanager ist heute kein Nice-to-have mehr – er ist ein essenzieller Pfeiler der Sicherheitsstrategie jedes Unternehmens. Denn in modernen Unternehmen mit hybriden Arbeitsmodellen, Cloud-Diensten und einer Vielzahl digitaler Anwendungen wird das Management von Passwörtern zur logistischen Herausforderung.

Foto: Fotocommunity, Illustration: Keeper Security

In vielen Unternehmen – etwa im Mittelstand mit verteilten Standorten und remote arbeitenden Teams – ist der Zugriff auf unterschiedliche Anwendungen wie CRM-Systeme, E-Mails oder interne Plattformen Alltag. Überall werden Logins benötigt und benutzt: oft über Jahre entstanden, nie vollständig dokumentiert und mit gefährlich einfachen Passwörtern.

Vor diesem Hintergrund ist es keine Frage, ob Unternehmen einen Passwortmanager nutzen sollten, sondern welchen. Keeper bietet hier eine Lösung, die über klassisches Passwortmanagement hinausgeht.



- **Neue Mitarbeitende erhalten automatisch einen eigenen, verschlüsselten Passwort-Tresor mit definierten Zugriffsrechten.**
- **Echtzeitüberwachung ermöglicht es der IT, unsichere oder kompromittierte Passwörter sofort zu identifizieren und gegenzusteuern.**
- **Mit der Dark-Web-Überwachung (BreachWatch) erkennt Keeper, ob Zugangsdaten geleakt wurden – noch bevor Schaden entsteht.**
- **Das Privileged Access Management (PAM) regelt zentral die Rechtevergabe für Admins, Dienstleister oder Projektmitarbeitende inklusive Live-Monitoring von Sessions.**
- **Besonders sensible Informationen wie API-Schlüssel oder Datenbank-Zugänge lassen sich im „Secrets Manager" sichern, einer Zero-Knowledge-Plattform für automatisierte Verwaltung und Rotation geheimer Daten.**

Single Sign-on: Weniger Reibung, mehr Sicherheit

Ein Mitarbeitender, der sich zehnmal täglich mit verschiedenen Passwörtern anmelden muss, greift oft zu einfachen, aber unsicheren Praxislösungen. Keeper begegnet diesem Risiko mit SSO Connect – einer Single-Sign-on-Integration, die bestehende Identitätsdienste wie Azure AD oder Okta einbindet. So genügt eine einmalige Anmeldung pro Tag. Mitarbeitende arbeiten sicher und komfortabel, während Keeper im Hintergrund den Zugriff schützt.

Schnelle Integration für jede IT-Landschaft

Keeper überzeugt durch seine cloudbasierte Architektur: Ohne lokale Infrastruktur, plattformunabhängig und webbasiert funktioniert die Integration schnell und unkompliziert – selbst bei heterogenen Strukturen oder BYOD-Konzepten.

Zentrale Steuerung – volle Kontrolle

Die zentrale Verwaltung ermöglicht IT-Abteilungen eine standortunabhängige Kontrolle über die Zugangsdaten. Dank Zero-Knowledge-Architektur hat Keeper keinen Zugriff auf die Inhalte – ideal für regulierte Branchen. Zugriffsrechte, Compliance-Status und Risiken lassen sich über Dashboards und Live-Monitoring jederzeit verfolgen.

Zero Trust als Sicherheitsprinzip

Keeper folgt dem Zero-Trust-Modell: Kein Nutzer oder System wird per se als vertrauenswürdig eingestuft. Zugriffe müssen stets eindeutig authentifiziert und autorisiert werden – ideal ergänzt durch Multi-Faktor-Authentifizierung und rollenbasierte Zugriffskontrolle. Das reduziert die Angriffsfläche maßgeblich.

Zukunftsfähige Sicherheit

Keeper beweist: IT-Sicherheit muss nicht kompliziert sein – aber umfassend. Die Plattform ist weit mehr als ein Werkzeug zur Passwortspeicherung – sie ist ein umfassendes Sicherheitssystem, das den modernen Anforderungen hybrider Arbeitswelten ebenso gerecht wird wie der zunehmenden Regulierung digitaler Geschäftsprozesse.

Foto: yubico

Der geschäftliche Nutzen auf einen Blick:

- Deutliche Reduktion von Helpdesk-Anfragen zu Passwortproblemen
- Erhöhte Produktivität durch schnellere Logins
- Minimierung des Risikos durch Credential Theft und Phishing
- Erfüllung von Compliance-Anforderungen (z. B. DSGVO, NIS2)
- Zentrale und einfache Verwaltung von Authentifizierungsmedien

Hardwarebasierte Authentifizierung mit FIDO2

Sicherer Zugang auch ohne Passwort

In Zeiten zunehmender Cyberkriminalität, wachsender regulatorischer Anforderungen und steigender Nutzererwartungen stehen IT-Verantwortliche und Entscheider unter Druck: Wie lässt sich der Zugriff auf Unternehmenssysteme nicht nur besser absichern, sondern auch unkomplizierter und komfortabler gestalten?

Schwache und wiederverwendete Passwörter zählen zu den größten Sicherheitsrisiken in Unternehmen – nicht zuletzt, weil sie Einfallstore für Phishing- und Malware-Angriffe darstellen. Die hardwaregestützte, passwortlose Zugriffskontrolle von FIDO2 bringt hier eine entscheidende Wende: Sie ersetzt Passwörter durch starke, asymmetrische Kryptografie, bei der der private Schlüssel sicher auf einem Hardware-Token, z. B. einem USB-Stick, gespeichert wird. Der dazugehörige öffentliche Schlüssel wird beim jeweiligen Onlinedienst hinterlegt. Ein unbefugter Zugriff auf den Account durch Phishing oder Datenlecks kann faktisch ausgeschlossen werden.

Ein Schlüssel für alle Anwendungen

Ein wesentlicher Vorteil liegt auch in der Alltagstauglichkeit: Für Endnutzer entfällt die ständige Passworteingabe. Mit einem einmal registrierten FIDO2-Token – z. B. einem YubiKey – genügt ein einfacher Fingertip, um sich sicher zu authentifizieren – intuitiv und plattformübergreifend, unterstützt durch Standards wie USB, NFC oder Bluetooth. Ein einziger FIDO2-Token kann für tausende Anwendungen genutzt werden – ob Cloud-Dienste, interne Web-Anwendungen oder Identity-Provider.

Maximale Sicherheit

Anders als bei klassischen Zwei-Faktor-Methoden mit SMS oder Apps, bei denen Codes auch über nicht sichere Kanäle übertragen werden, basiert FIDO2 vollständig auf Public-Key-Kryptografie. Dies schützt nicht nur vor Phishing, Replay- und Man-in-the-Middle-Angriffen, sondern eliminiert auch das Risiko durch gestohlene Zugangsdaten aus anderen Diensten, denn jeder Service nutzt sein eigenes Schlüsselpaar. Selbst wenn ein Angreifer Zugang zu einem kompromittierten Dienst erhält, kann er die gestohlenen Daten nicht für den Zugriff auf andere missbrauchen.

Skalierbar von 2FA bis zu Hochsicherheitsanwendungen

FIDO2 bietet eine Sicherheitsarchitektur, die unterschiedlichen Anforderungen gerecht wird. Vom Single-Factor-Login über das klassische Zwei-Faktor-Login (2FA) bis zur komplexen Multi-Faktor-Authentifizierung sorgt FIDO2 für erhöhte Sicherheit und schützt sensible Informationen. Dies qualifiziert die Public-Key-Kryptografie der passwortlosen Zugriffskontrolle unter anderem für den Einsatz in Umgebungen mit hohen Compliance-Anforderungen. Große Plattformen unterstützen FIDO2 bereits nativ und der offene Standard ermöglicht eine breite Kompatibilität etwa mit Active Directory, Azure AD und Google Workspace, was die Integration in bestehende IT-Infrastrukturen erleichtert. ■

Hardware-Token und YubiKey

Ein Hardware-Token ist ein physisches Gerät, das zur Authentifizierung in digitalen Systemen verwendet wird. Es generiert entweder zeitlich begrenzte Einmalpasswörter (OTP) oder wird via USB, NFC oder Bluetooth direkt mit einem Gerät verbunden. Ein solches Hardware-Token ist zum Beispiel der YubiKey des schwedischen Unternehmens Yubico: ein USB-Stick, der eine Zwei- oder Multi-Faktor-Authentifizierung durch das Einstecken in einen USB-Port oder durch NFC ermöglicht. Da der YubiKey ein einmaliges Passwort generiert, bietet er einen effektiven Schutz vor Phishing oder anderen Strategien zur Kaperung von Passwörtern.

Kaspersky Security Awareness Plattform

IT-Sicherheit beginnt beim Menschen

Illustration: Kaspersky

Wenn es um die IT-Sicherheit von Unternehmen geht, stellt sich nicht nur die Frage nach leistungsstarken Firewalls oder aktuellen Virenscannern. Viel entscheidender ist oft: Wie gut sind Mitarbeitende geschult mit digitalen Gefahren umzugehen? Hier setzt die Kaspersky Security Awareness Plattform an: mit einem durchdachten Weiterbildungsprogramm, das Mitarbeiter befähigt, aktiv zur Cybersicherheit beizutragen.

Spätestens seit der Corona-Pandemie ist der Arbeitsplatz nicht mehr zwangsläufig das Büro – eine Entwicklung, die Cyberkriminelle gezielt ausnutzen. Denn dezentral organisierte IT-Strukturen mit privaten Netzwerken bieten mehr Angriffspunkte. Die Awareness Plattform von Kaspersky trägt dieser neuen Realität Rechnung, indem sie auch Szenarien im Homeoffice berücksichtigt und für Schwachstellen sensibilisiert.

Komplexe Bedrohung, wirksame Prävention

Phishing-E-Mails, unsichere Passwörter und sogenannte Social-Engineering-Tricks gehören längst zum Standardrepertoire digitaler Angreifer. Besonders perfide: Angriffe, bei denen Kriminelle versuchen, über Mitarbeiter Vertrauen zu erschleichen und so in Unternehmensnetzwerke einzudringen. Oft genügt ein Klick auf einen scheinbar harmlosen Link, um einen Totalausfall der IT oder den Verlust sensibler Daten zu verursachen. Die Schulungsplattform von Kaspersky vermittelt genau hierfür das nötige Wissen – praxisnah, situationsbezogen und interaktiv.

Lernen, erleben, handeln – mit Edutainment

Im Zentrum der Kaspersky-Plattform steht das Prinzip des spielerischen Lernens („Edutainment“). Mitarbeiter durchlaufen in wenigen Minuten reale Alltagssituationen – etwa das Erkennen einer Phishing-Seite oder wichtige Entscheidungen im Umgang mit sensiblen Daten. Statt trockener Theorie setzt Kaspersky auf interaktive Module, Online-Planspiele und praxisorientierte Tests. Ein Beispiel: In einem kurzweiligen Test mit zwölf Szenarien prüfen User in 15 Minuten ihr Gespür für IT-Risiken – die Ergebnisse liefern Hinweise auf mögliche Wissenslücken.

Individuell, skalierbar, messbar

Die Kaspersky Security Awareness Plattform ist modular aufgebaut und lässt sich auf Unternehmen jeder Größenordnung und Branche anpassen – ohne umfangreiche Vorbereitungen oder externe Beratungsleistungen. Besonders betont wird die Messbarkeit des Lernerfolgs: Fortschritte werden dokumentiert, Wissenslücken sichtbar gemacht und der Lernerfolg aktiv gesteuert.

Führungskräfte als Vorbild

Ein nachhaltiger Sicherheitsansatz funktioniert nicht ohne die Unterstützung des Managements. Kaspersky bezieht daher ausdrücklich auch Führungskräfte mit ein – mit spezialisierten Szenarien, in denen Entscheidungsträger in simulierten Geschäftsumgebungen auf reale Cyberbedrohungen reagieren müssen. Ziel ist es, das Sicherheitsbewusstsein auf allen Unternehmensebenen zu verankern.

IT-Sicherheit ist Teamarbeit

Angesichts aktuell zunehmender digitaler Bedrohungen wird deutlich: Ein gut geschultes Team ist der beste Schutz gegen Cyberangriffe. Die Kaspersky Security Awareness Plattform zeigt, wie sich durch systematisches, interaktives Training eine sicherheitsbewusste Unternehmenskultur aufbauen lässt. Unternehmen, die auf Prävention setzen und ihre Mitarbeiter aktiv in ihre Sicherheitsarchitektur einbinden, verschaffen sich einen klaren Vorteil bei der Abwehr von Cyberattacken. ■

Impressum

Redaktion: Karl-Heinz Zonbergs

Herausgeber: Mario Hösel (V.i.S.d.P.)
Fernmelde- & Computerservice Hösel
Blumenstraße 1
09526 Olbernhau
Telefon(0 37 360) 69 08-0
Telefax(0 37 360) 69 08-50
Internet: www.fernmeldeservice.de
E-Mail: info@fernmeldeservice.de

Layout: Ulrike Hartdegen
E-Mail: layout@ulrikehartdegen.de

Anschrift der Redaktion:
BestWord
Kappenstraße 70
45473 Mülheim an der Ruhr
Telefon (02 08) 76 24 99
Telefax (02 08) 76 23 92
E-Mail: info@bestword.de