Lesen Sie mehr unter **unternehmensratgeber.info**

Schutz und Sicherheit

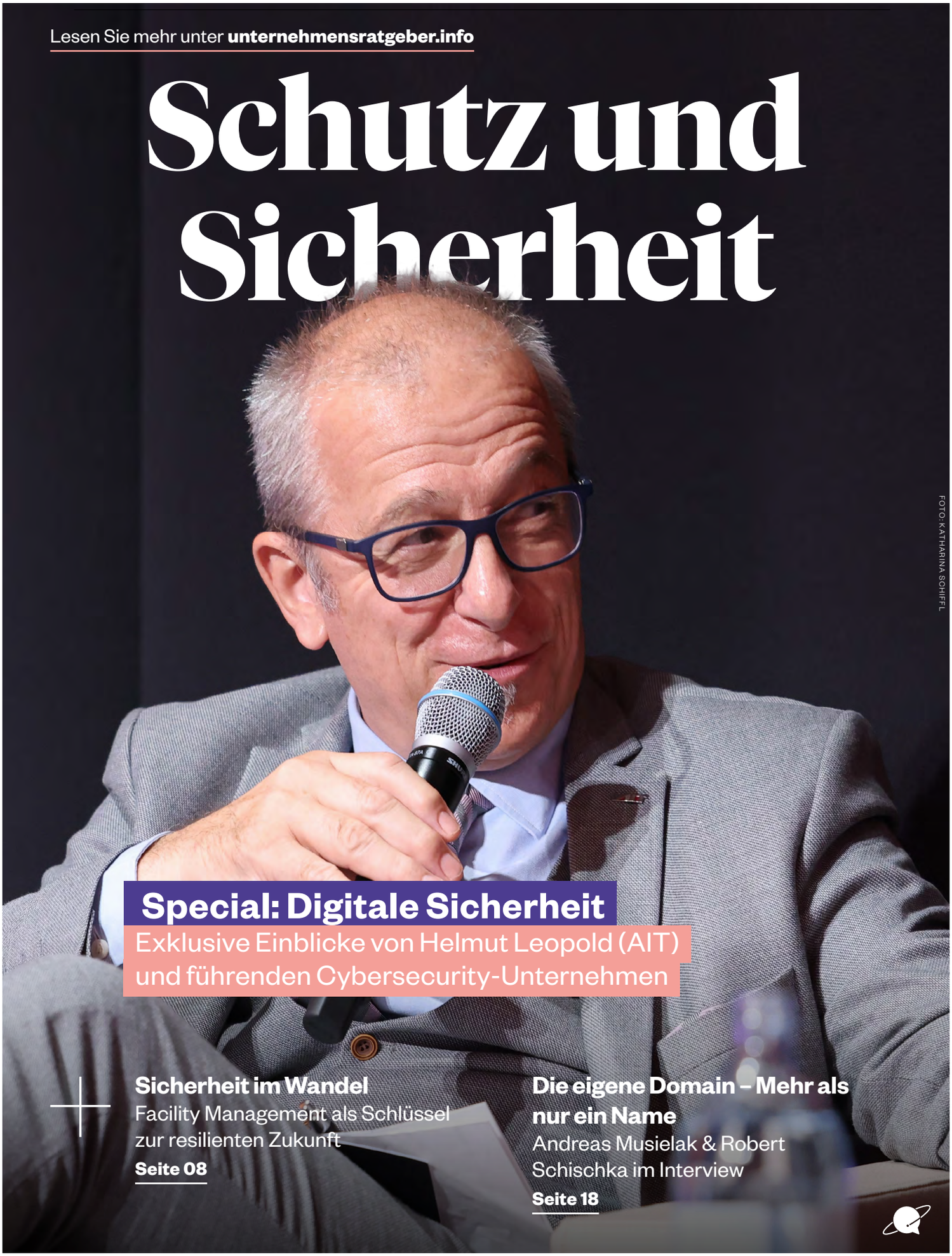


FOTO: KATHARINA SCHIFFL

Special: Digitale Sicherheit

Exklusive Einblicke von Helmut Leopold (AIT) und führenden Cybersecurity-Unternehmen

Sicherheit im Wandel
Facility Management als Schlüssel zur resilienten Zukunft
Seite 08

Die eigene Domain – Mehr als nur ein Name
Andreas Musielak & Robert Schischka im Interview
Seite 18

IN DIESER AUSGABE

Project Manager: **Stefan Lemmerer, BSc**
Business Developer: **Paul Pirkelbauer, BA**
Lektorat: **Sophie Müller, MA**
Grafik und Layout: **Juraj Prikopa**
Managing Director: **Bob Roemké**
Fotocredits: **wenn nicht anders angegeben bei Shutterstock**

Medieninhaber: **Mediaplanet GmbH, Bösendorferstraße 4/23 · 1010 Wien · ATU, 4759844 · FN 322799f FG Wien**
Impressum: **mediaplanet.com/at/impressum/**
Distribution: **Der Standard Verlagsgesellschaft m.b.H.**
Druck: **Mediaprint Zeitungsdruckerei Ges.m.b.H. & Co.KG**

Kontakt bei Mediaplanet: Tel: **+43 676 847 785 256**
E-Mail: hello-austria@mediaplanet.com ET: **11.09.2025**

Bleiben Sie in Kontakt:

Mediaplanet Austria
@mediaplanet.austria

VORWORT

Sehr geehrte Leser:innen!

„Sicherheit ist nicht alles, aber ohne Sicherheit ist alles nichts“ – Ich stelle dieses Zitat, das oft mit einem einfachen mundartlichen „Jo eh“ oder „Eh klar“ quittiert wird, ganz bewusst an den Beginn dieses Vorworts zum Thema Schutz und Sicherheit.


FOTO: HBF

General Rudolf Striedinger
Generalstabschef des Österreichischen Bundesheeres

Bundesministerium Landesverteidigung

Und ich lade dazu ein, sich Gedanken darüber zu machen, mit welcher Selbstverständlichkeit wir die Sicherheit, in der wir leben, als gegeben annehmen. Oft ist uns nicht bewusst, wer dafür welchen tagtäglichen Aufwand zu leisten hat, um dies zu gewährleisten.

Wie selbstverständlich gehen wir davon aus, dass morgens Strom aus der Steckdose kommt, um Kaffee zuzubereiten; oder Warmwasser aus dem Duschkopf – damit wir den Tag gemäß unseren Vorstellungen beginnen können.

Ebenso selbstverständlich sind für uns Funktionsfähigkeit und Sicherheit unserer Technologien und technischen Geräte wie Handy, Notebook und Software, die wir täglich nutzen. Nicht mehr ganz so viel Selbstverständlichkeit bringen wir jedoch für unser persönliches – das richtige – Verhalten auf, um unsere Daten und Informationen, vor allem online, zu schützen.

In Bezug auf die Sicherheit im öffentlichen Raum, beispielsweise im Straßenverkehr, sind wir uns unserer aktiven Beteiligung bewusst. Wir müssen unseren Beitrag leisten, verlassen uns jedoch auch hier auf unsere Mitmenschen. Wir versuchen, Regeln einzuhalten – hoffen aber auch darauf, dass Ordnungshüter:innen für unsere Sicherheit sorgen, damit wir uns frei bewegen können.

Sicherheit und Freiheit stehen also in engem Zusammenhang. Und unsere Freiheit – das Privileg, in einem demokratischen Rechtsstaat leben zu können – sollten wir schätzen. Hierfür gilt es, einzutreten und sich zu engagieren.

Für unsere Freiheit und Sicherheit in Österreich leistet auch das Bundesheer seinen Beitrag, indem es das Land unter anderem gegen alle militärischen Bedrohungen von außen schützt und gegebenenfalls verteidigt. Dies ist jedoch nicht alleine Aufgabe des Bundesheeres – die umfassende Landesverteidigung sieht eine Reihe von Aufgaben und Verantwortlichkeiten vor.

Tragen wir also alle dazu bei – jede:r für sich und gemeinsam –, dass wir als Staat und Gesellschaft in Frieden und Freiheit auf demokratischer Basis unter Berücksichtigung unserer Werte zusammenleben können.

Die nachfolgenden Beiträge stellen dafür eine gute Basis und Wissensbereicherung dar.

Ich lade Sie herzlich ein, die Lektüre Schutz und Sicherheit aufmerksam zu lesen – es zahlt sich aus! ■

Ihr
Rudolf Striedinger

EXPERTISE

Zivilschutz Österreich

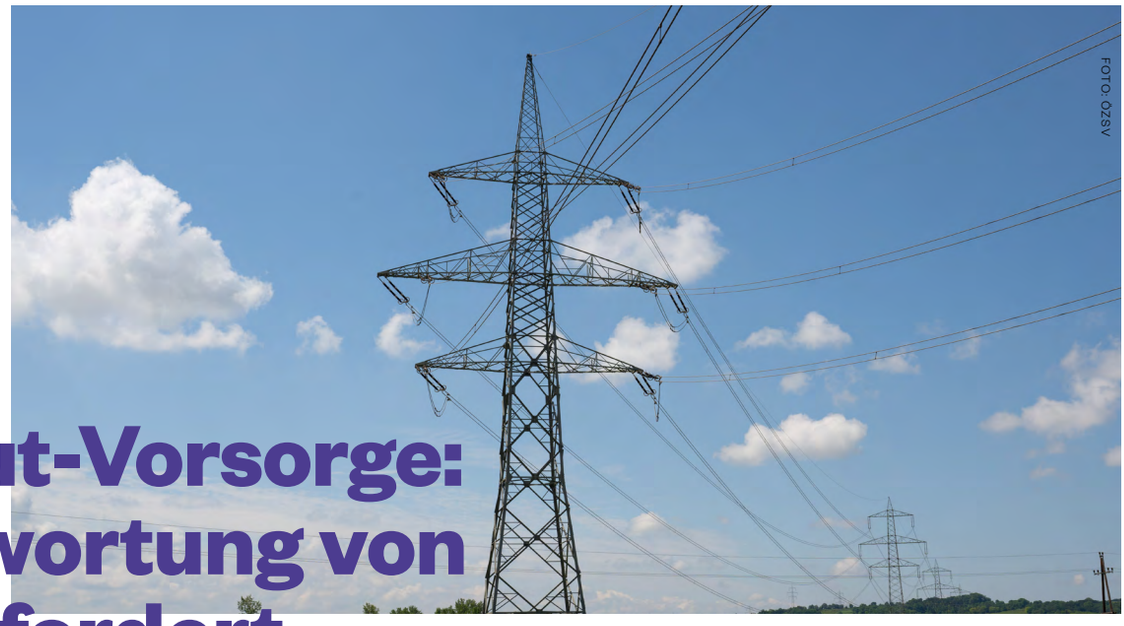


FOTO: ÖZSV

Blackout-Vorsorge: Verantwortung von allen gefordert

Ein plötzlich eintreffendes Blackout, wie ein großflächiger und gravierender Stromausfall genannt wird, ist kein Katastrophenszenario aus einem Film, sondern eine reale Bedrohung. Nicht zuletzt die Ereignisse auf der Iberischen Halbinsel Anfang dieses Jahres zeigten, dass solche Szenarien ohne Vorankündigung jederzeit eintreten können und über Ländergrenzen hinweg zu einem totalen Stillstand führen. Je länger ein Blackout anhält, desto gravierender sind die Effekte auf Gesellschaft und Wirtschaft.

Private Vorsorge: einfache Schritte mit großer Wirkung

Jede und jeder kann durch einfache Maßnahmen zur eigenen Sicherheit beitragen. Der Zivilschutzverband empfiehlt eine Notbevorratung an Lebensmitteln und Getränken sowie Hygieneartikeln und Medikamenten für den persönlichen Gebrauch. Unverzichtbar sind außerdem Taschenlampen, Batterien sowie ein batterie- oder mit Kurbel betriebenes Radio, um im Anlassfall informiert bleiben zu können. „Erstellen Sie Ihren individuellen Plan für den Fall eines Blackouts und besprechen Sie diesen mit Ihrem Umfeld“, empfiehlt Andreas Hanger, Präsident des Zivilschutzverbandes, denn „Vorsorge ist kein Luxus, sondern unsere gemeinsame Verantwortung. Wer vorbereitet ist, schützt nicht nur sich selbst, sondern auch seine Mitmenschen.“

Unternehmen in der Pflicht

Neben Haushalten stehen auch Unternehmen und Institutionen vor Herausforderungen bei der Vorbereitung auf ein mögliches Blackout. Zuerst gilt es zu definieren, ob - und wenn ja, welche - Abläufe im Anlassfall aufrechterhalten werden müssen. So haben etwa ein Modegeschäft oder eine Kreativagentur andere Notwendigkeiten wie Betriebe der Lebensmittelversorgung, des Gesundheitswesens oder im Transport- und Logistikbereich. Hier sind unterbrechungsfreie Prozesse essenziell und die vergangenen Jahre zeigten anschaulich, welche Auswirkungen die Unterbrechung von Lieferketten haben. Notfallpläne, die Schulung von Mitarbeiter:innen und die Sicherstellung kritischer Abläufe gehören im Anschluss daran zu einer professionellen Vorbereitung.

Der Zivilschutzverband als Partner in der Vorsorge

Der Zivilschutzverband unterstützt mit seinen Informationsangeboten, Vorträgen und Schulungen für Mitarbeiter:innen bei der Vorbereitung auf Katastrophenszenarien – seien es ein Blackout oder Extremwetterereignisse. Kern seiner Arbeit ist dabei die Bewusstseinsbildung über mögliche Risiken und die Vermittlung von einfach umzusetzenden Vorsorgemaßnahmen. Damit wird der wesentliche Grundstein für die Resilienz des eigenen Unternehmens gesetzt, denn nur wenn ausreichend individuelle Vorsorge getroffen wurde, stehen Mitarbeitende auch im Anlassfall zur Verfügung.

Neue Herausforderungen durch Digitalisierung

Stürme, Cyberangriffe oder technische Störungen können jederzeit Dominoeffekte auslösen. Mit zunehmender Digitalisierung, Elektromobilität und internationalen Lieferketten steigt die Abhängigkeit von einer stabilen Energieversorgung. Auch Homeoffice, digitale Verwaltungsprozesse oder bargeldloses Zahlen machen uns verwundbarer. Umso wichtiger ist es, dass Vorsorge auf allen Ebenen ernst genommen wird – von der privaten Wohnung bis zum global agierenden Konzern.

Denn am Ende ist Blackout-Vorsorge Teamarbeit: Jede und jeder kann einen Beitrag leisten egal ob Bürger:in oder Unternehmen. „Wer heute vorsorgt, ist morgen resilienter und stärkt damit die Sicherheit der gesamten Gesellschaft“, appelliert Zivilschutz-Präsident Hanger. ■


FOTO: PAUL GRUBER

Andreas Hanger
ÖZSV-Präsident

Nähere Informationen finden Sie unter: www.zivilschutz.at

FOTO: VAS

Digitale Schutzausrüstung im Jahr 2025: Intelligenter Schutz für moderne Arbeitswelten

Die Arbeitswelt verändert sich rasant – digitale Technologien durchdringen sowohl Produktionsprozesse als auch Logistik und Servicebereiche. Auch die persönliche Schutzausrüstung (PSA) bleibt davon nicht unberührt. PSA 4.0 ist keine Zukunftsvision mehr, sondern bereits gelebte Praxis. Sie schützt nicht nur, sondern analysiert, warnt und kommuniziert – und das alles in Echtzeit.

Was ist digitale PSA?
Die digitale PSA umfasst Ausrüstungen wie Helme, Handschuhe, Brillen oder Schutzkleidung, die mit Sensoren und Aktoren ausgestattet sind. Diese erfassen Vitaldaten, Bewegungsprofile, Umwelteinflüsse und Nutzungsmuster. Die Informationen werden über smarte Plattformen oder Apps verarbeitet und ausgewertet. Ziel ist eine proaktive Gefahrenvermeidung statt eines nur reaktiven Schutzes. PSA 4.0 erkennt etwa Hitzestress, warnt bei Schadstoffbelastung oder gibt bei einem Sturz automatisch eine Notfallmeldung ab.

Der digitale Arbeitsplatz – vernetzt und adaptiv
Cyber-physische Systeme (CPS) prägen zunehmend die Arbeitsumgebung: Vernetzte Maschinen, smarte Werkzeuge und digitale PSA bilden gemeinsam ein intelligentes Sicherheitsnetz. PSA wird dadurch zum integralen Bestandteil von Prozesssteuerung, Zugangskontrolle und Gesundheitsmonitoring.

Vernetzte Arbeitssicherheit
Der österreichische Verband zur Förderung der Arbeitssicherheit (VAS) ist ein Netzwerk aus 41 namhaften Unternehmen, die persönliche Schutzausrüstung herstellen, vertreiben oder servicieren. Ziel ist es, Wissen und Innovationen aus der Branche zu bündeln und branchenübergreifend zugänglich zu machen. Im Fokus stehen die Qualität, Sicherheit und digitale Zukunft der PSA. Das Netzwerk entwickelt gemeinsam Standards, fördert den Erfahrungsaustausch und setzt Impulse für die Weiterentwicklung von PSA 4.0 in der Praxis. Durch Veranstaltungen, Fachforen und Arbeitsgruppen trägt der VAS maßgeblich zur Professionalisierung der Arbeitssicherheit bei.

MASon App – Neuigkeiten, Tools und Safety-Pedia
Die MASon App des VAS ist die zentrale digitale Plattform für Informationen, Tools und Fachwissen rund um persönliche Schutzausrüstung. Nutzer:innen erhalten regelmäßig Updates aus der PSA-Branche, aktuelle Produktinfos und praxisnahe Inhalte. Herzstück der App ist die sogenannte Safety-Pedia – ein kontinuierlich wachsendes digitales Nachschlagewerk zu Begriffen, Normen und Anwendungen in der Arbeitssicherheit. MASon verbindet Wissen mit Weiterbildung und ist damit ein kompaktes Werkzeug für Sicherheitsfachkräfte, Einkäufer:innen und Anwender:innen von PSA.

Chancen und Risiken
Die Vorteile liegen auf der Hand: höhere Sicherheit, schnellere Reaktionen, genauere Analysen und bessere Einbindung der Beschäftigten. Besonders bei PSA der Kategorie III (z. B. Atemschutz) schafft die Kombination mit digitalen Systemen eine neue Qualität der Absicherung. Aktuell noch nicht vollständig geregelt sind Herausforderungen wie Datenschutz, Systemzuverlässigkeit und rechtliche Verantwortlichkeiten.

Digitale PSA – Technik oder persönliche Maßnahme?
Mit der Integration von digitaler PSA in Unternehmensnetzwerke stellt sich außerdem folgende arbeitsrechtliche Frage: Ist PSA 4.0 weiterhin ‚persönlich' oder bereits ein Teil der Technik im Sinne der klassischen Schutzmaßnahmen-Hierarchie? Die Antwort wird künftig Einfluss auf Haftung, Investitionsentscheidungen und Schulungspflichten haben.

Fazit
PSA 4.0 ist heute gelebte Realität. Voraussetzung bleibt ein ganzheitlicher Zugang: technische Ausstattung, klare Datenstrategie, Schulung der Beschäftigten – und Mut, Sicherheitsarbeit neu zu denken. ■

MASon
Die News-App rund um Arbeitssicherheit für iOS und Android. Hier geht's zum Download:

Persönliche Schutzausrüstung: Sicherheitsseile, die Leben schützen

Mag. Florian Teufelberger leitet sein Familienunternehmen, die Teufelberger Holding AG, bereits in der siebten Generation. Im Interview erklärt er gemeinsam mit Produktmanager für Persönliche Schutzausrüstung (PSA) gegen Absturz, Roland Ecker, wie wichtig es ist, für jede Anwendung das passende Sicherheitsseil zu nutzen. Und auch das Training für die richtige Anwendung der PSA darf nicht zu kurz kommen.

FOTO: TEUFELBERGER

Roland Ecker
Head of S&S PPE

FOTO: TEUFELBERGER

Florian Teufelberger
Geschäftsführer

Welche Rolle spielen Schutz und Sicherheit in Ihrer langen Unternehmensgeschichte?
FT: Schutz und Sicherheit stecken in unserer DNA. Ein 85-jähriger Seilmacher, der bei einem Meister gelernt hatte, der bei meinem Urgroßvater Martin Teufelberger in die Lehre gegangen war, erzählte mir einmal, dass er sich als junger Handwerker weigerte, einem Kunden eine Wäscheleine zu verkaufen, und deshalb Ärger bekam. Dabei hatte er das Richtige getan, denn der Kunde wollte ‚mit der Wäscheleine seine Frau am Berg absichern'. Mit dieser Geschichte macht mich der alte Seilmacher stolz, denn sie belegt, dass unser Verständnis von Sicherheit tief in uns verankert ist – und wir das auch vermitteln und somit Schutz bewirken.

Was bedeutet Sicherheit für Teufelberger konkret?
FT: Sicherheit hat für uns seit unserer Unternehmensgründung im Jahr 1790 immer zwei Seiten: Wir Seilhersteller:innen verantworten sowohl die Qualität unserer Seile in der Herstellung als auch die sachgerechte Handhabung durch unsere Kunden.

Ihre Produkte sichern Menschen und Lasten weltweit. Haben Sie ein Beispiel für ein weniger bekanntes Einsatzgebiet, wo Teufelberger zur Sicherheit beiträgt?
RE: Seil ist für uns nicht gleich Seil: Vielmehr ist jedes Seil ein Konstrukt aus spezifischen Komponenten, die erst im Zusammenspiel ihr Sicherheitspotenzial entfalten. Es kommt immer auf die Fasern und ihre Verarbeitung im Kern und Mantel des Seils an. Wir haben zum Beispiel das erste Faserseil für Kräne entwickelt. Ein noch recht frischer Erfolg ist unsere aufwändige Entwicklung eines Seils mit deutlich dünnerem Durchmesser von 6 mm statt bislang 8 – 11 mm, das für den Notfall als Bergungsseil in den Gondeln von Windkraftanlagen gesetzmäßig vorhanden sein muss. Der geringere Durchmesser unseres neuen Seils spart Gewicht und Platz – bei zugleich sicherer Anwendung.

Was zeichnet Teufelberger im Bereich PSA gegen Absturz aus?
RE: Wir achten im Beratungsgespräch genau darauf, wie ein Seil angewendet werden soll, wählen das aus unserer Erfahrung passende Seil aus und schulen die Anwender:innen im unternehmenseigenen Trainingszentrum darin, es sicher einzusetzen. Unsere Halle bietet hierfür realitätsnahe Bedingungen mit Leitern, Schacht, Dach und Kranausleger.

Warum ist es wichtig, nicht nur Sicherheitsprodukte anzubieten, sondern auch entsprechende Trainings mit Fachpersonal für die Anwender:innen?
RE: Nicht allen ist sofort bewusst, wie wichtig das Training ist. Wenn wir mit einer Puppe einen Absturz simulieren, wird jedoch auch den Letzten klar, dass selbst das stabilste Halteseil allein nicht vor dem Fall schützt. Es braucht immer auch eine sichere Verbindung zum Gurtsystem und eine geschulte Hand, die das Ganze sicher im Griff hat.

Wir nehmen das P in der Bezeichnung PSA sehr ‚persönlich': Denn die sicherste Schutzausrüstung ist immer zugeschnitten auf die Person, die sie nutzt. Das heißt, die Passgenauigkeit der Seile, Gurte etc. ist uns ebenso wichtig wie der fachgerechte Umgang damit. Unsere Trainer:innen sind alle im Bereich Industrieklettern ausgebildet und vermitteln ihre jahrelange Praxiserfahrung.

Sicherheit, Nachhaltigkeit und Innovation wachsen immer stärker zusammen – welche Entwicklungen sind in den nächsten Jahren relevant?
FT: Das Thema Rohstoffe beschäftigt uns seit unserer Gründung – es ging und geht immer darum, noch stabilere, schnittfestere, hitzebeständigere, feuerfestere, leichtere und längere Seile zu entwickeln. Heute sind wir auf das dünne 6-mm-Seil zu Recht stolz. In 30 Jahren sagen wir rückblickend vielleicht: ‚Wie lieb, 6mm! Wir wussten es damals nicht besser!' Die Wahl der Rohstoffe für unsere Seile ist immer auch eine Frage der Nachhaltigkeit: Schon heute können wir einen Teil unserer Seilfasern recyceln und wiederverwenden. Unser Ziel ist ein vollständig geschlossener Rohstoffkreislauf. ■

Lesen Sie mehr unter: www.teufelberger.com/de/

Digitale Identität: Sind Sie sicher, dass Sie Sie sind?

Österreich gilt als Vorreiter in Europa, was die digitale Identität angeht. Mit seinem bereits im Echtbetrieb laufendem digitalen Führerschein ist das Land derzeit sogar an der Spitze der EU[1]. Aber: Eine digitale Identität braucht Absicherung, denn Identitätsdiebstahl und Datenmissbrauch sind eine ernste Bedrohung für jede:n. Wie sich die digitale Identität absichern lässt, steht hier.

Text
Doreen Brumme

In analogen Zeiten gaben Eltern ihrem Nachwuchs eigene Vornamen sowie den Familiennamen. Damit war der Grundstein für eine eigene Identität gelegt. Diese wurde in der Geburtsurkunde festgeschrieben und später samt persönlichen Merkmalen wie Augenfarbe und Größe auf den Personalausweis übertragen. Jede:r war dank des Profils auf den Dokumenten überall eindeutig identifizierbar. Mittlerweile dreht sich die Welt jedoch digital und die Menschen sind nicht mehr nur offline, sondern auch online unterwegs – mit ihrer digitalen Identität.

Was Ihre digitale Identität ist und wie Sie sie sich zulegen

Ganz gleich, wo Sie sich im Internet bewegen: Sie zeigen sich dort immer mit Ihrer digitalen Identität. Diese ergibt sich aus Ihren Profildaten, die Sie beim Registrieren eingeben, wenn Sie Onlineangebote wie E-Mailing, Online-Banking, E-Learning, Online-Dating, Online-Shopping, E-Meldewesen, E-Gesundheitswesen oder Social Media nutzen wollen. Benutzername, Passwort und Anschrift werden so zum Schlüssel in die digitale Welt. Über diesen werden Sie für die Dienstanbietenden eindeutig er- und wiedererkennbar. Viele Dienste verknüpfen mit den von Ihnen eingegebenen Daten zudem Informationen über Sie, die sie aus der Beobachtung Ihres Nutzer:innenverhaltens gewinnen.

Grundsätzlich kommen Sie auf dreierlei Weise an Ihre digitale Identität:

1. **Amtliche Login:** In Österreich ist die ID Austria (eID) Ihr amtliches Signaturwerkzeug. Sie ist EU-weit anerkannt und wird bereits von 4,1 Millionen Österreicher:innen genutzt[2]. EU-weit wird dafür das einheitliche „European Digital Identity (EUDI)"-Wallet (Brieftasche) gemäß der „Electronic Identification, Authentication- and Trust-Services"-Verordnung (eIDAS 2.0) aufgebaut – damit Sie sich in der EU digital ausweisen und Verträge rechtsgültig unterzeichnen können.
2. **Föderierte Login:** Die Möglichkeit, dass Sie sich hier und dort via Apple, Google oder LinkedIn anmelden, fußt auf Standards wie OpenID Connect beziehungsweise SAML im Unternehmensumfeld. Ein sogenannter Identity Provider (IdP) bestätigt dabei gegenüber einer Webseite (Relying Party), wer Sie sind.
3. **Selbstbestimmte und Wallet-basierte Login:** Hier erhalten Sie digitale Nachweise wie den Studierendenausweis in eine Wallet-App und zeigen selektiv nur notwendige Daten vor. Das Ganze beruht auf Webstandards wie W3C Verifiable Credentials und dezentralen Kennungen (DID).

Was Ihnen Ihre digitale Identität bringt – und was Sie Ihnen schlimmstenfalls nimmt

Ihre digitale Identität verschafft Ihnen den berechtigten Zugang zu Angeboten im Internet. Sie können beispielsweise „Behördengänge" machen, um eine neue Adresse zu melden, einen Ausweis zu beantragen oder Steuern zu zahlen. Die digitalen Amtswege sind kürzer als die analogen, rund um die Uhr geöffnet und von überallher erreichbar – Sie sparen dank dessen jede Menge Lebenszeit.

Zugleich geht mit der digitalen Identität jedoch ein Sicherheitsrisiko einher: Denn Identitätsklau und Datenmissbrauch sind in digital eine viel größere Bedrohung als in analog. Sie verlieren im Ernstfall nicht nur den berechtigten Zugriff auf Ihre digitalen Serviceplattformen – auch Schadensbegrenzung und Strafverfolgung sind in einem die ganze Welt umspannenden Internetz schwieriger.

Wie sicher Ihre digitale Identität ist – und wie Sie sie noch sicherer machen

100-prozentige Sicherheit vor Identitätsdiebstahl und Datenmissbrauch gibt es weder in der analogen noch der digitalen Welt. Das wissen die Menschen laut einer aktuellen Studie[3]. Dennoch gibt es oft ein Knowing-Doing-Gap zwischen der Sorge um die Sicherheit und individuell zu treffenden Schutzmaßnahmen wie:

1. Verwenden einzigartiger, langer Passwörter und 2-Faktorauthentifizierung
2. regelmäßiges Updaten des Betriebssystems und Browsers
3. Gerätesperre per PIN und/oder Biometrie

Sie sehen: Eine sichere digitale Identität ist der Boden, auf dem Vertrauen und Akzeptanz in der digitalen Gesellschaft sprießen. Entscheidend für ihr weiteres Gedeihen ist, dass Sicherheit und Nutzerfreundlichkeit zusammenspielen. ■

[1] www.staatsdruckerei.at/allgemein/oesterreich-erfuellt-eu-vorgaben-fuer-digitalen-fuehrerschein-vorzeitig/
[2] www.oe24.at/oesterreich/politik/4-1-millionen-nutzen-id-austria-jetzt-will-proell-alle-oesterreicher-im-system/643300902
[3] www.ots.at/presseaussendung/OTS_20250904_OTS0056

Vom Wachssiegel zum digitalen Ausweis - Sichere Identität made in Austria

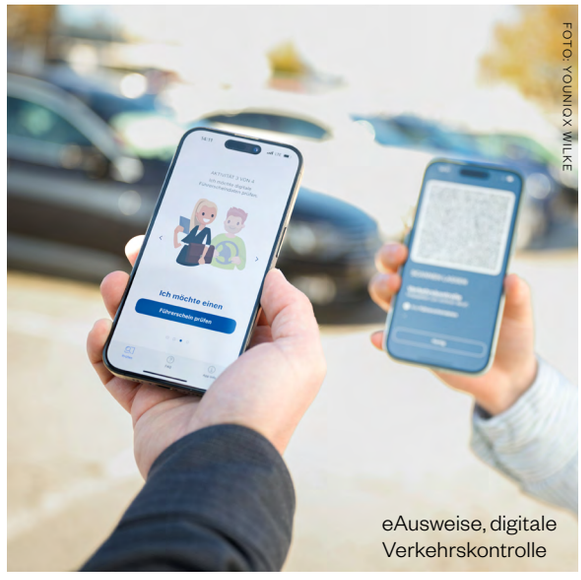


FOTO: YOUNIQX/WILKE

eAusweise, digitale Verkehrskontrolle

Mit einer Geschichte von über 220 Jahren zählt die Österreichische Staatsdruckerei (OeSD) zu den traditionsreichsten Unternehmen Österreichs. Seit der Gründung durch Kaiser Franz I. hat sich aber nicht nur das politische und gesellschaftliche Umfeld grundlegend gewandelt, sondern auch die zentralen Tätigkeitsfelder der Staatsdruckerei: Von den Anfängen mit Passierscheinen, Briefmarken und Wachssiegeln hat sich das Unternehmen zu einem heute führenden Experten für modernen Hochsicherheitsdruck und sichere digitale Identitäten entwickelt.

Neben der laufenden Weiterentwicklung bei Sicherheitsmerkmalen von Reisepass, Personalausweis und Co. setzte die OeSD-Gruppe auch früh auf sichere digitale Identität. Bereits 2015 stellte das Unternehmen die weltweit erste Smartphone-App "MIA – My Identity App" für elektronische Identität und digitale Ausweise vor. "Für uns war klar, dass moderne digitale Identität die Sicherheit und Einfachheit in der Benutzung in den Fokus stellen muss", unterstreicht OeSD Generaldirektor Helmut Lackner. Seit 2017 bündelt die OeSD-Gruppe ihre Expertise zu digitaler Identität in der hauseigenen Softwareschmiede "youniqx Identity".

Digitale eAusweise: sichere digitale Ausweise als App

Die Erfahrungen als Pionier in digitaler Identität setzte die Digitaltochter der OeSD bereits in mehreren Projekten erfolgreich um. So ist die youniqx Identity der verantwortliche Entwickler für die österreichische "eAusweise"-App mit digitalen Ausweisen wie dem digitalen Führer- und Zulassungsschein, dem digitalen Altersnachweis und dem digitalen Identätsnachweis.

Grenzüberschreitender Einsatz durch EUDI

Einen weiteren Meilenstein für digitale Ausweise markiert die aktuelle Entwicklung der EUDI Wallet ("EU Digital Identity"). Entsprechend EU-Rechtsvorgaben sollen die EU-Mitgliedsstaaten zukünftig kompatible digitale Ausweise bereitstellen. Nach der Umsetzung sollen diese Ausweislösungen dann in der gesamten EU gelten. Das bedeutet, dass digitale Ausweise wie beispielsweise der österreichische digitale Führerschein in Zukunft auch im EU-Ausland anerkannt sein werden.

Mehr Sicherheit durch digitale Identität

Diese Entwicklung schafft nicht nur mehr Sicherheit für den Bürger, sondern auch für die Wirtschaft. So verweist Lackner auf einen kürzlichen Hack in Italien, bei dem fast 100.000 Scans von Reisepässen und Personalausweisen von Hotelgästen in die falschen Hände gelangten. "Durch digitale Ausweise werden unsichere Kopien von Reisepässen überflüssig. Beim Checkin in einem Hotel oder auch beim Mieten eines Mietwagens wäre es schon heute möglich, einfach ihren digitalen Ausweis per Knopfdruck herzuzeigen", führt Lackner aus. Durch entsprechende Softwareanbindungen könnten Firmen nach der expliziten Zustimmung des Nutzers die notwendigen Daten direkt in die eigenen Firmensysteme übernehmen. "Keine Formulare, keine Scans. Das reduziert den Zeitaufwand für beide Seiten und sorgt für mehr Sicherheit gegen Betrug und Identitätsdiebstahl". Zusätzlich ist dieser Prozess auch von Grund auf datenminimierend. "Statt mit einem Scan alle Daten des Identitätsdokuments zu übermitteln, können bei digitalen Ausweisen nur die wirklich notwendigen Daten digital übermittelt werden. Damit ist dieser Vorgang von Grund auf datenminimierend", erklärt Lackner die Hintergründe.

Österreich als Vorreiter

Durch den Echtbetrieb von digitalen Ausweisen bietet sich in Österreich aktuell eine einmalige Möglichkeit an. "Unternehmen können in Österreich schon heute Erfahrungswerte für den gesamten EU-Markt sammeln, die ab 2026 dann in allen 27 Mitgliedsstaaten und somit für fast 450 Millionen EU-Bürger eingesetzt werden könnten", führt Lackner aus. Damit ist sichere digitale Identität nicht nur eine Notwendigkeit zum Schutz der höchstpersönlichen Identität, sondern gleichzeitig ein Wettbewerbsvorteil für jene Unternehmen, die schon jetzt in die Zukunft von digitaler Identität investieren möchten. ■

Lesen Sie mehr unter staatsdruckerei.at

EXPERTISE

FMA IFMA Austria Chapter

Sicherheit im Wandel – Facility Management als Schlüssel zur resilienten Zukunft

Sicherheit im Facility Management ist heute mehrdimensional. Sie entsteht nicht allein durch bauliche Maßnahmen oder technische Systeme, sondern durch das Zusammenspiel von Digitalisierung, Nachhaltigkeit, Nutzer:innenbewusstsein und intelligenter Gebäudetechnologie. Nur wenn diese Aspekte ineinandergreifen, entsteht ein wirklich sicheres Umfeld – heute und für kommende Generationen.

FOTO: FMA I IFMA AUSTRIA, JANA MADZIGON

Adrian Jamrozowicz
Abteilungsleiter Technisches Gebäudemanagement, Aquila Hausmanagement GmbH

Smart Buildings und das Internet of Things (IoT) ermöglichen dabei eine neue Qualität der Gebäudesicherheit. Sensoren, vernetzte Systeme und automatisierte Abläufe liefern in Echtzeit Daten über Zutritt, Klima, Energieverbrauch und sicherheitsrelevante Zustände. Diese Informationen werden über zentrale Plattformen wie PSIM-Systeme (Physical Security Information Management) gebündelt und analysiert – zunehmend unterstützt durch Künstliche Intelligenz (KI). So lassen sich Risiken frühzeitig erkennen, Prozesse optimieren und Entscheidungen datenbasiert treffen.

Doch Technik allein schafft keine Sicherheit. Auch das Sicherheitsbewusstsein muss aktiv gefördert werden – bei Betreiber:innen, Dienstleister:innen und Nutzer:innen. Facility Management kann hier gezielt Programme initiieren, die informieren, sensibilisieren und zur Mitverantwortung motivieren. Denn Sicherheit entsteht dort, wo Menschen eingebunden sind und verstehen, wie sie selbst zum Schutz beitragen können.

Gleichzeitig ist Nachhaltigkeit ein unverzichtbarer Bestandteil moderner Sicherheitsstrategien. Energieeffiziente Systeme, ressourcenschonende Prozesse und umweltfreundliche Materialien tragen nicht nur zum Klimaschutz bei, sondern erhöhen auch die Resilienz von Gebäuden – etwa durch bessere Luftqualität, geringere Brandlasten oder stabile Versorgungssicherheit. Nachhaltige Lösungen wirken nicht nur heute, sondern schützen auch die Generationen von morgen.

Facility Management ist zum zentralen Dreh- und Angelpunkt für Sicherheit im umfassenden Sinn geworden. Es vereint bauliche Stabilität mit digitaler Intelligenz, stärkt gesellschaftliches Vertrauen und fördert nachhaltige Entwicklung. Die Herausforderung liegt darin, diese Dimensionen nicht isoliert, sondern als ein integriertes System zu verstehen – mit dem Ziel, Räume zu schaffen, die sicher, lebenswert und zukunftsfähig sind. ■

Adrian Jamrozowicz hat sich in seiner Diplomarbeit intensiv mit dem Thema Gebäudesicherheit auseinandergesetzt. Im Rahmen seiner Forschung zur „Analyse des Verbesserungspotenzials der physischen Gebäudesicherheit durch Einführung eines Sicherheitsleitstandes (PSIM) in Bestandsgebäuden“ konnte er wertvolle Erkenntnisse gewinnen und die Jury des Future-Talent-Awards 2025 der FMA I IFMA Austria, des österreichischen Netzwerks für Facility Management, überzeugen.

Future-Talent-Award
der FMA I IFMA Austria – Jetzt einreichen!

Haben auch Sie eine Abschlussarbeit zum Thema Facility oder Property Management geschrieben? Egal ob klassisches Gebäudemanagement, smarte Infrastrukturservices, Sanierung, Digitalisierung oder nachhaltige FM-Konzepte – wir suchen Ideen, die unsere Branche weiterbringen.

Bei uns haben wissenschaftliche Arbeiten genauso Platz wie Projekte direkt aus der Praxis. Besonders freuen wir uns über Beiträge mit Nachhaltigkeitsbezug, denn die Zukunft braucht Lösungen, die nicht nur clever, sondern auch verantwortungsvoll sind.

Einmal pro Jahr verleihen wir den Future-Talent-Award und holen damit die besten Arbeiten vor den Vorhang. Nutzen Sie die Chance, Ihre Forschung sichtbar zu machen und die Zukunft des Facility Managements mitzugestalten!

Einreichungen zum Future-Talent-Award 2026 sind bereits unter www.fma.or.at möglich.

Lesen Sie mehr unter
www.fma.or.at

EVENTS

imh KONFERENZEN SEMINARE Wissen, das bewegt

Zertifizierter Intensivlehrgang Datenschutz
07.10.2025 - 09.10.2025
www.imh.at/datenschutz-intensiv
Wien

Datenschutz in der Forschung und Lehre
13.10.2025 - 14.10.2025
www.imh.at/datenschutz-fog
Renaissance Wien Hotel, Wien

11. Jahrestagung Datenschutz
21.10.2025 - 22.10.2025
www.imh.at/datenschutz
Austria Trend Park-hotel Schönbrunn, Wien

Datenschutz Update
laufend
www.imh.at/datenschutz-online
online

Datenschutz BrushUp
04.12.2025
www.imh.at/dsgvo-brushup
online

WEKA AKADEMIE

Neuregelungen im Chemikalienrecht
06.10.2025
Online
www.forum-akademie.at/neuregelungen-im-chemikalienrecht/

Technisches Risikomanagement im Unternehmen
11.11.2025
ARCOTEL Wimberger
www.forum-akademie.at/technisches-risikomanagement-im-unternehmen/

Special: Digitale Sicherheit

FOTO: KATHARINA SCHIFFL

Cyberangriffe zählen heute zu den größten Risiken für Unternehmen und Gesellschaft. Gleichzeitig entstehen innovative Lösungen, um Schutz und Vertrauen zu stärken. In den folgenden Seiten präsentieren namhafte Cybersecurity-Unternehmen ihre Expertise und Lösungen. Zudem geben die Experten Helmut Leopold und Christoph Schmittner Einblicke in aktuelle Herausforderungen und zukünftige Entwicklungen.

NTS RELAX, WE CARE

Digitale Resilienz mit NTS

Cyberangriffe werden immer raffinierter, regulatorische Anforderungen strenger und IT-Landschaften komplexer. Um den Geschäftsbetrieb im Ernstfall aufrechtzuerhalten, braucht es umfangreiche Schutzmaßnahmen. Ein nahtloses Zusammenspiel auf technischen und organisatorischen Ebenen ist entscheidend: NTS unterstützt seine Kunden hierbei mit individuell zugeschnittenen Lösungen für echte digitale Resilienz.

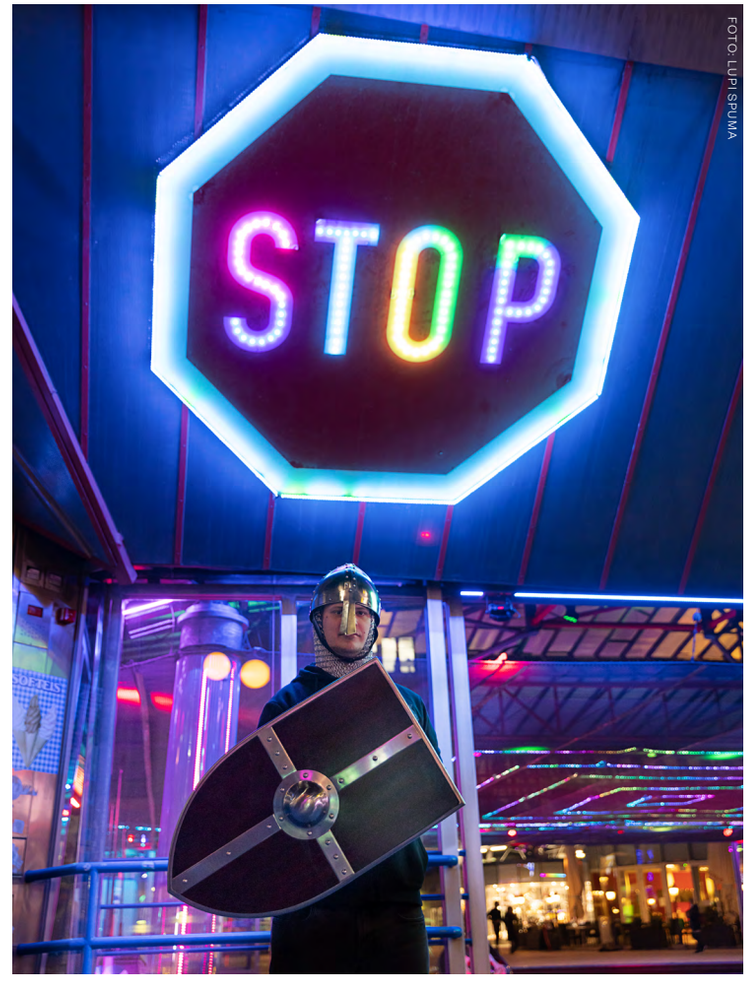


FOTO: LUPI SPUMA

Sicherheit von Grund auf

Ein zentrales Element zur Verbesserung der digitalen Resilienz ist die europäische NIS 2 Richtlinie, die die Anforderungen an Cybersicherheit deutlich verstärkt. Am Beginn steht aber ein konsequentes Vulnerabilitätsmanagement. Vor allem bei bekannten Lücken geht es um die möglichst rasche Schließung. Weiters müssen Prozesse etabliert und klare Verantwortlichkeiten geschaffen werden. Das bedeutet Risiken nicht nur reaktiv zu behandeln, sondern auch proaktiv für dauerhafte Grundsicherheit zu sorgen. Hier setzt NTS mit dem Vulnerability Management Service an: Schwachstellen werden erkannt, bewertet und priorisiert, sowie notwendige Maßnahmen rechtzeitig umgesetzt.

Auch ein robuster Perimeterschutz bleibt unverzichtbar. Er bildet die erste Verteidigungslinie und blockiert unerwünschten oder sogar gefährlichen Datenverkehr bereits am Eingang. Auch wenn sich durch Cloud, mobile Arbeit etc. die Grenzen eines Netzwerks verschoben haben, bleibt dieser Schutzwall zentral in modernen Sicherheitsarchitekturen. NTS unterstützt mit NG-Firewalls, SSE- und SASE-Lösungen sowie DNS-Security. Darüber hinaus übernimmt NTS Betriebsverantwortung durch Managed Infrastructure Security Services. Gemeinsam mit starken Partnern wird so eine kontinuierlich aktualisierte Abwehr aufgebaut.

Mit der Cloud-Nutzung muss auch die digitale Identität der Nutzer:innen in der Schutzstrategie beachtet werden. NTS bietet Multi-Faktor-Authentifizierung, adaptive Zugriffskontrollen und individuelle Zero-Trust-Konzepte. Damit wird verhindert, dass gestohlene Zugangsdaten oder kompromittierte Konten zum Einfallstor für Angriffe werden.

Angriffe erkennen und reagieren

Falls es doch zu einem Cybersecurity Vorfall kommt, ist es entscheidend, Bedrohungen frühzeitig zu erkennen und gezielt darauf zu reagieren. NTS bietet den Threat Detection Service, der Daten aus verschiedensten Quellen sammelt, korreliert und in Echtzeit analysiert und auf einer hochautomatisierten Plattform basiert. Security Analyst:innen kümmern sich um potenzielle Incidents und bieten Kund:innen damit ein SOC-as-a-Service. Ergänzend unterstützt das Incident Response Service bei der schnellen Eindämmung und Analyse von Sicherheitsvorfällen.

NTS begleitet Unternehmen bei der Umsetzung ganzheitlicher Maßnahmen mit einem umfassenden Security Services Portfolio. Dabei kommen innovative Produkte und Technologien starker Partner zum Einsatz, die durch jahrzehntelange Erfahrung zu maßgeschneiderten Lösungen werden. Das Ergebnis: Sicherheit, die den Betrieb im Alltag schützt - echte digitale Resilienz. ■

Lesen Sie mehr unter: www.nts.eu/security/

NTS - RELAX, WE CARE

Mit dieser Motivation übernehmen wir Verantwortung und gestalten und betreuen IT-Lösungen mit Sorgfalt, Qualität und zertifizierter Erfahrung. Unsere technische Leidenschaft, gepaart mit Super Services, sorgt für begeisterte Kunden und langjährige Partnerschaften. Gemeinsam mit ausgewählten High-End-Herstellern kreieren wir Lösungen für Network, Security, Collaboration, Cloud und Data Center.
Die NTS Netzwerk Telekom Service AG mit Hauptsitz in Graz wurde 1995 von den Eigentümern Alexander Albler und Hermann Koller gegründet. Derzeit sind rund 878 Mitarbeitende an 22 Standorten weltweit beschäftigt.
www.nts.eu

Entgeltliche Einschaltung

ZETTASECURE
CYBERSECURITY MIT DURCHBLICK

Cybersecurity – mit 24/7-Monitoring machbar

Der Geschäftsführer der Zettasecure GmbH, Wien, Philipp Mandl, klärt über die aktuelle Bedrohungslage im Cyberspace auf und beschreibt, was der Einsatz externer Cybersecurity-Profis insbesondere kleineren Unternehmen bringt – Spoiler: hohe IT-Sicherheit zu überschau- und planbaren Kosten.

FOTO: ZETTASECURE

Philipp Mandl
Geschäftsführer
Zettasecure

Warum ist Cybersecurity für jedes Unternehmen ein Muss?
Weil sie über den Geschäftserfolg entscheidet. Cybersecurity schützt vor Cyberangriffen, die 2025 zahlreich – wir reden von mehreren Millionen Standardblocks im Monat – aus unterschiedlichen Richtungen kommen: von kriminellen Netzwerken, staatlich unterstützten Akteur:innen, Hacktivist:innen und automatisierten, KI-gestützten Angreifer:innen. Laut der Studie Cybersecurity in Österreich* ist jeder siebte Cyberangriff hierzulande erfolgreich. Die Bedrohung ist also real.

Dabei geht es heute nicht mehr nur um Datendiebstahl oder Erpressung mittels Ransomware, sondern auch um das Manipulieren ganzer Geschäftsprozesse. Der Druck auf Unternehmen wächst: Sie müssen ihre und die Systeme ihrer Businesspartner:innen absichern. Bei jedem dritten Unternehmen kommt es zum Schaden, weil Lieferant:innen oder Dienstleister:innen Opfer von Cyberangriffen sind.*

Mit welchen Schäden ist bei solchen Angriffen zu rechnen?
Ein gelungener Cyberangriff, der auf das wertvollste Gut des Unternehmens, seine Daten, abzielt, verursacht beispielsweise Geldverluste. Hierfür habe ich ein konkretes Beispiel aus unserer Praxis: Unternehmen X übermittelte Rechnungen und wunderte sich, dass sein Kunde nicht zahlte. Nach erhaltener Mahnung rief der Kunde an und konnte nachweisen, dass er längst bezahlt hatte. Doch was war passiert? Ein Angreifer hat sich in den Rechnungsversand eingeklinkt und eine manipulierte Rechnung mit seiner eigenen Kontonummer versendet.

Doch davor kann man sich schützen, indem eine Funktion oder ein Prozess ins System integriert wird, die bei jeder Zahlung die verifizierte und hinterlegte IBAN der Zahlungsempfänger:innen mit der auf der aktuellen Rechnung vergleicht. Der Kunde wäre demnach beim Versuch, die ‚falsche IBAN' ins Überweisungsformular einzugeben, alarmiert worden. Gefahr erkannt – Gefahr gebannt.

Erfolgreiche Cyberangriffe stören nicht nur den Betrieb, denn schlimmstenfalls kommt er zum Erliegen (Betriebsausfall). Das schadet der Wettbewerbsfähigkeit und zieht finanzielle Verluste nach sich. Und auch die Tatsache, Opfer eines Cyberangriffs geworden zu sein, spricht sich früher oder später herum. Für Kund:innen kann das ein Grund sein, dem Unternehmen künftig nicht mehr zu vertrauen. Sie gehen schlussendlich zur Konkurrenz (Kundenverlust). Kommt es wegen ungenügender Absicherung zu Sicherheitsverstößen oder werden gesetzliche Vorschriften nicht eingehalten, drohen Strafzahlungen, die schnell in die Millionen gehen.

Wie sicher ist gut ausgebaute Cybersecurity – und was kostet sie?
Hundertprozentige Cybersecurity gibt es nicht. Aber: Wer sie mitdenkt und umsetzt, kann sich in hohem Maß absichern. 80 Prozent der Cybersecurity lassen sich inhouse erreichen, das kostet nichts extra. Dabei geht es vor allem um saubere Softwareinstallationen und regelmäßige Updates derselben. Mangelhafte Updates waren für jedes 4. Unternehmen in der oben bereits erwähnten Studie Auslöser für erfolgreiche Cyberangriffe.* 17 - 18 weitere Prozent der Cybersecurity können ebenso inhouse oder mit externen Profis erreicht werden, üblicherweise zu durchaus günstigen Konditionen. Die übrigen 2 bis 3 Prozent sind aufwendiger, weil sie von Expert:innen umgesetzt werden müssen und dadurch entsprechend teurer sind.

Wo liegt die Herausforderung für Unternehmen?
Viele investieren in angemessenem Umfang in ihre IT. Doch eine IT, die das eigens aufgesetzte System gegen Cyberangriffe absichern soll, ist wie eine Steuerberatung, die ihre Wirtschaftsprüfung selbst macht: betriebsblind. Hier passieren unweigerlich Fehler, die jedoch erst auffallen, wenn ein Cyberangriff schon geglückt und der Schaden längst entstanden ist.

Wir schaffen Cybersecurity als externes und unabhängig zertifiziertes Security Operations Center (SOC) unter anderem mit unseren Managed Security Services (MSS), die auch ein Rund-um-die-Uhr-Monitoring umfassen. Je nach Stundenbudget unterscheiden sich unsere Reaktionsmodi (24/7 oder 8/5) und die umfassende Betreuung. Ungewöhnliche Aktivitäten erkennen wir frühzeitig und stoppen sie effizient. Das ist insbesondere für kleinere und mittlere Unternehmen interessant, die sich eine teure Inhouse-Cybersecurity nicht leisten können oder wollen. Die Services sind dabei bereits ab 400 € pro Monat verfügbar, was sie zu einer leistbaren und professionellen Lösung macht. ■

Erfahren Sie mehr unter
zettasecure.com

*https://kpmg.com/at/de/home/insights/2025/05/cybersecurity-studie-2025.html

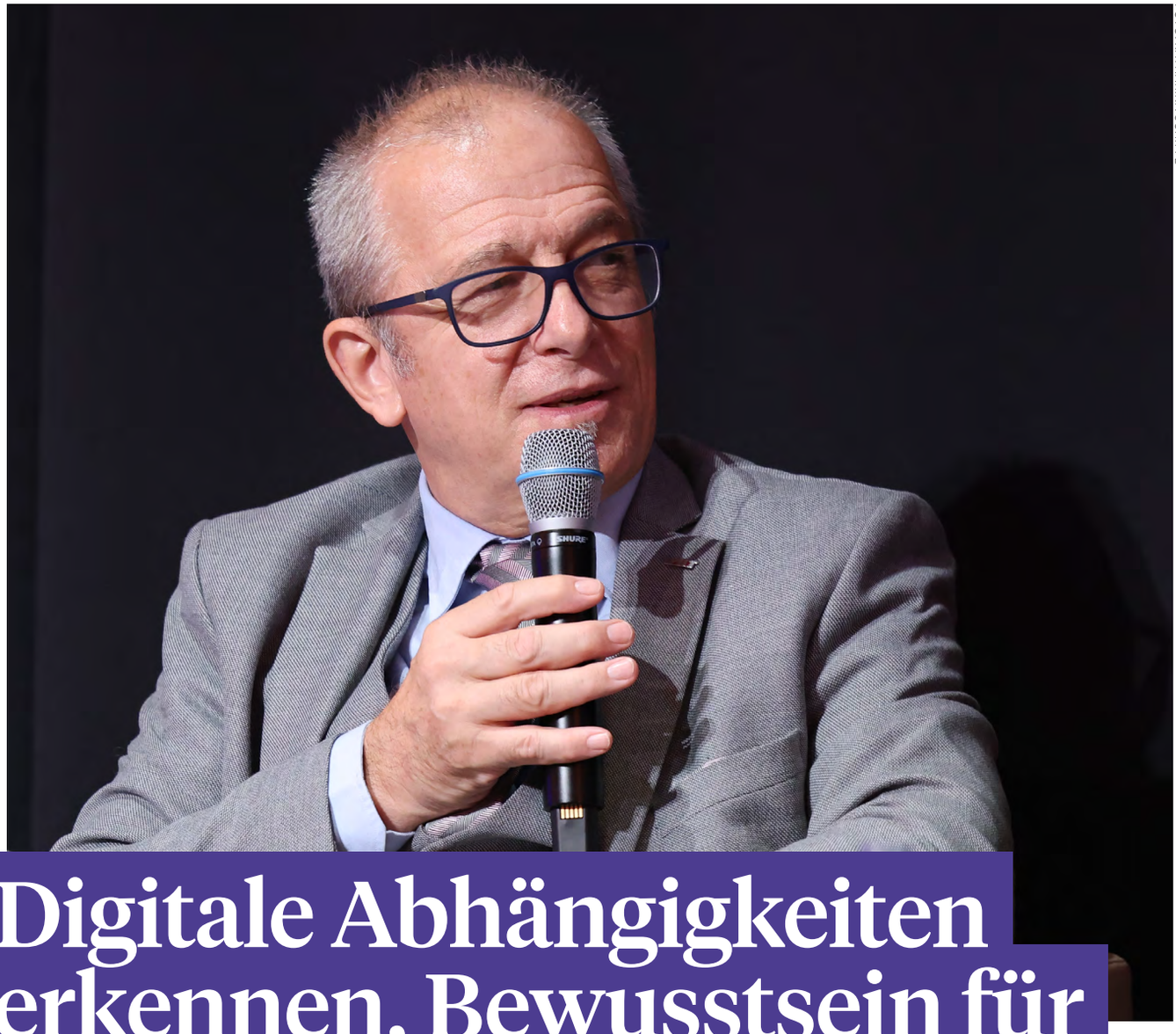


FOTO: KATHARINA SCHIFFL

Digitale Abhängigkeiten erkennen, Bewusstsein für Datensouveränität stärken

Das Internet und die vielen smarten Anwendungen für Kommunikation, Datenübertragung und Informationsverarbeitung – aber auch zur Steuerung und Wartung von Industrieanlagen – haben im digitalen „always-on"-Zeitalter den globalen Cyberspace geformt. Er ist damit zur unentbehrlichen Grundlage für die Wirtschaft sowie für unser gesellschaftliches Miteinander geworden. Und schließlich sind durch diese umfassende Vernetzung von Menschen und Maschinen zu smarten Systemen neue datengetriebene Geschäftsmodelle und faszinierende Anwendungen von künstlicher Intelligenz (KI) entstanden.

FOTO: JOHANNES ZINNER

DI Helmut Leopold PhD
Head of Center for Digital Safety & Security

Es ist uns jedoch noch viel zu wenig bewusst, dass wir durch diese Entwicklung in eine maßgebliche Abhängigkeit geschlittert sind. Unsere funktionierende Wirtschaft, unser gesellschaftliches Leben und unsere staatliche Administration sind ohne intakte digitale Infrastrukturen mittlerweile undenkbar geworden.

Gleichzeitig sind wir mit einer rasant wachsenden Cyber-Kriminalität konfrontiert: Immer wieder neue Beispiele erfolgreicher Angriffe auf Computer und IT-Systeme führen zu beträchtlichen persönlichen oder wirtschaftlichen Schäden. Die Bandbreite der Angriffsmethoden über Telefonnetze und Internet ist groß: Ausspionieren persönlicher Bankdaten, Betrug beim Online-Shopping, Angriffe auf Unternehmen und Produktionseinrichtungen, um Lösegeld zu erpressen oder Unternehmensgeheimnisse auszuspionieren, oder Angriffe auf Unternehmen, kritische Infrastrukturen und staatliche Einrichtungen aus terroristischen Motiven. Dabei ermöglicht die mittlerweile einfache Verfügbarkeit von KI, die Angriffsmethoden nun noch ausgeklügelter durchzuführen. KI hilft den Angreifer:innen, Schwachstellen in digitalen Systemen zu finden, entwirft Bedienungsanleitungen, um Datendiebstähle und Systemeinbrüche einfacher und schneller durchzuführen oder erzeugt täuschend echt wirkende Texte, Bilder, Videos und Sprachnachrichten, um uns Nutzer:innen von IT-Systemen zu täuschen oder zu manipulieren. Außerdem hilft unsere bedenkenlose Nutzung von weit verbreiteten KI-Anwendungen Angreifer:innen letztlich, da jeder Prompt gleichzeitig Training für die KI bedeutet. So gelangt sie einfach an Unternehmens- und Privatdaten und lernt sogar Abläufe von Unternehmensprozessen.

Um in dieser Digitalwelt unsere IT-Systeme besser zu schützen braucht es ein radikales Umdenken:

- Cyber-Sicherheit muss als strategisches Thema auf Geschäftsführungsebene positioniert sein.
- Eine effiziente, an aktuelle Bedingungen angepasste Cyber-Sicherheitshygiene ist erforderlich. Diese umfasst geeignete Unternehmensprozesse und IT-Architekturen, die Verwendung von Firewalls, Virenschutz und Backup-Systemen und Zutrittsschutzkonzepte.
- Essenziell ist ebenso das vollumfängliche Schaffen und die Steigerung des Bewusstseins für Cyber-Sicherheitsbedrohungen in Unternehmen bei allen Benutzer:innen von IT-Systemen.

Damit die Wirtschaft und Staaten vor den wachsenden globalen Bedrohungen durch Cyber-Kriminalität und Terrorismus geschützt sind, müssen darüber hinaus neue Sicherheitsstandards und Regulierungen in den Unternehmen und Behörden umgesetzt werden.

Dementsprechend betrifft das kommende NIS-2 Gesetz zum Schutz kritischer Infrastrukturen alle Unternehmen, die einen wesentlichen Einfluss auf die nationale Wirtschaft oder Gesellschaft haben. Energieversorger:innen, Serviceanbieter:innen, öffentliche Dienstleister:innen und auch große Produktionsbetriebe müssen ihre Cyber-Sicherheit weiter erhöhen und organisatorische Fähigkeiten entwickeln, um Cyber-Angriffe rasch identifizieren und Informationen zur Bildung von nationalen Cyber-Sicherheits-Lagebildern für die Behörden zur Verfügung stellen zu können. Die persönliche Haftung der Geschäftsführung ist dabei für die Einhaltung des NIS-2 Gesetzes wesentlich.

Der ebenfalls neue Cyber Security Act (CSA) verlangt ab 2027 verbindlich eine Zertifizierung aller digitalen Produkte, um eine höhere Cyber-Sicherheit bei allen Produktlösungen und in System-Zulieferungsketten sicherzustellen. In ähnlicher Weise gibt es bereits neue Vorgaben in der Automobilindustrie, die umfassende Änderungen in den Prozessen der Produktentwicklung für die Zulieferer:innen bedeuten.

Zur Einhaltung all dieser Regulierungen und Gesetze zur Abwehr von Cyber-Bedrohungen stehen neueste Forschungsergebnisse und Innovationen made in Austria zur Verfügung, z. B.:

- Security by Design: Digitale Systeme müssen schon im Designprozess einem Risikomanagementprinzip folgen, d. h. von vornherein so gebaut werden, dass sie höchst widerstandsfähig gegenüber Sicherheitsbedrohungen sind.
- Einsatz von KI als Schutzsystem: IT-Systeme müssen in der Lage sein, Angriffsversuche automatisch zu erkennen.
- Einsatz von starken, quantensicheren Verschlüsselungssystemen zum Schutz unserer Daten auch vor zukünftigen Bedrohungen durch einen Quantencomputer: Österreich und die EU haben hier eine internationale technologische Führungsrolle eingenommen.

Schließlich braucht es unbedingt die Entwicklung von organisatorischer Expertise durch fortlaufende Ausbildungs- und Trainingsmaßnahmen für alle Mitarbeiter:innen, um auf den Ernstfall vorbereitet zu sein. Moderne Schulungsanbieter:innen arbeiten mit „Cyber Ranges“, um die Abwehr von Cyber-Angriffen realitätsnah zu simulieren und zu trainieren. Auch in diesem Bereich hat Österreich eine internationale Vorreiterrolle übernommen. Das AIT Austrian Institute of Technology betreibt weltweit die Aus- und Weiterbildung zur IT-Sicherheit für kritische Infrastrukturbetreiber:innen im Auftrag der UN-Atomenergiebehörde (IAEA).

Fazit: Es ist ein rasches Weiterdenken notwendig, um Cyber-Sicherheit und Datensouveränität eine größere Bedeutung zu verleihen und sich so rechtzeitig auf die neuen Entwicklungen am Markt und im digitalen Raum vorzubereiten. ■

Österreich im Bereich der Digitalisierung nur im europäischen Mittelfeld

Manfred Koller, Business Development Manager Network & Security bei der ACP Gruppe, erklärt welche Vorteile das neue Cloud Rechenzentrum von Microsoft in Österreich bringt und welche Herausforderungen bei der digitalen Transformation bestehen.

FOTO: ACP

Manfred Koller
Business Development Manager Network & Security

Stichwort „digitale Transformation" – Wie weit sind heimische Unternehmen?
Während große Unternehmen sehr weit sind, besteht bei der Mehrzahl – Österreich ist schließlich ein KMU-Land – noch Aufholbedarf. Denn im Gegensatz zu global aufgestellten Großunternehmen fehlt es den vorwiegend kleineren und mittleren Unternehmen meist an Know-how und Fachkräften.

Welche Herausforderungen bringt die Digitalisierung noch mit sich?
Der Mittelstand spürt den wachsenden Druck, die Digitalisierung voranzutreiben – auch sie wollen von der Cloud und KI profitieren. Doch vor der Verbesserung unternehmerischer Prozesse gilt es das Netzwerk für die Nutzung der Cloud zu modernisieren und sämtliche Aktivitäten im digitalen Raum abzusichern. Die meisten Unternehmen wissen, dass sie im Bereich Cybersecurity und Netzwerk etwas tun müssen – die Frage ist nur, was?

Ich ziehe hier gerne den Vergleich mit einer Burg aus dem Mittelalter: Sie hatte eine Mauer und einen Graben zum Schutz. Die Zugbrücke wurde nur heruntergelassen, wenn man wusste, wer aus- und einfuhr. In vergangenen analogen Zeiten agierten Unternehmen ähnlich autark – sie waren lauter einzelne Burgen. Mit der Digitalisierung hat sich das grundlegend geändert: Unternehmen sind mit Lieferanten, Businesspartnern, und Dienstleistern vernetzt. Und auch die Mitarbeiter:innen arbeiten nicht mehr nur vor Ort, sondern auch im Homeoffice und remote. Das heißt, dass Zugriffe auf Unternehmensdaten und -ressourcen von überall aus erfolgen – und Sicherheit und Netzwerkdesign angepasst werden müssen.

Was können Unternehmen nun konkret tun?
Um das Unternehmen für die Nutzung der Cloud und die neue hybride Arbeitswelt fit zu machen, muss sichergestellt werden, dass der Zugriff auf Applikationen und Daten in der Cloud nicht nur performant, sondern auch sicher ist. Zum Beispiel durch Multifaktor Authentisierung und bedingte Zugriffsrechte auf Applikationen und Daten.

Hier sollte man unseren Spezialisten vertrauen, denn kein Unternehmen gleicht dem anderen. Wir kümmern uns um die Verbesserung des Sicherheitslevels, das Erreichen von relevanten Sicherheitsstandards wie NIS2 und bieten eine 24/7 Überwachung durch unser Security Operation Center (SOC). Und sollte doch etwas passieren, reagieren wir blitzschnell. Bereits über 140 Kunden nutzen unsere skalierbaren Services.

Wir schulen die Belegschaft anhand von Cybersecurity-Awareness-Trainings, führen Penetrationstests durch und passen die Sicherheitslevel entsprechend der Ergebnisse an. Zudem gibt es von uns ein IT-Notfallhandbuch, damit die Unternehmen bei einem Cyberangriff wissen, was zu tun ist.

Wir helfen den Unternehmen auch bei der Migration in die Cloud. Als Experten in dem Bereich war es uns wichtig als Launch Partner der Microsoft Cloud Region East dabei zu sein.

Was ist die österreichische Cloud-Region? Welche Vorteile bringen lokalisierte Cloud-Services?
Das im Juni im Raum Wien eröffnete Microsoft Rechenzentrum bedeutet, die Datenhaltung, -speicherung und -verarbeitung findet hier statt. Das bringt neben einem Geschwindigkeitsvorteil auch einen Sicherheitsvorteil, da die österreichische Cloud den lokalen Anforderungen an digitale Sicherheit (DSGVO, NIS2) gerecht wird.

Welche Rolle spielt ACP in der Partnerschaft mit Microsoft?
Wir arbeiten seit unserer Gründung eng mit Microsoft zusammen und besitzen umfangreiches Know-how, um Unternehmen Schritt für Schritt durch den Digitalisierungsprozess zu begleiten und sind ihr verlässlicher Umsetzungspartner.

„Wir freuen uns, gemeinsam mit starken Partnern wie ACP daran zu arbeiten, die digitale Transformation in Österreich zu beschleunigen. Cybersicherheit ist heute die Grundlage für zukünftiges Wachstum und damit ein wirtschaftlicher Erfolgsfaktor. Wenn Unternehmen Innovation nutzen wollen, brauchen sie ein stabiles, sicheres Fundament. Mit der Microsoft Cloud-Region bieten wir unseren Kund:innen sichere und leistungsstarke Cloud-Services aus Österreich – mit höchsten Sicherheits- und Datenschutzstandards und für alle Branchen und Unternehmensgrößen.", Diana Stoica, Security Lead bei Microsoft Österreich

Wie kommen Unternehmen in die österreichische Cloud?
Nach einer umfassenden Analyse finden wir maßgeschneiderte Lösungen für sie, weil wir die Unternehmen dort abholen, wo sie in Sachen Digitalisierung stehen. Mit dem österreichischen Cloud Rechenzentrum von Microsoft haben wir nun ein attraktives Cloud Service Angebot aus Österreich für Österreich. ■

Lesen Sie mehr unter
acp-gruppe.com

Mehr Infos zum Event ACP Security Inslider 2025

EXPERTISE

Security by Design: Pflicht, Chance und Herausforderung

Mit dem Cyber Resilience Act (CRA) erweitert die EU das bekannte CE-Kennzeichen. Ab 12. Dezember 2027 müssen Produkte mit digitalen Elementen cybersicher sein. Für Nutzer:innen ist die Botschaft eindeutig: Ein CE-gekennzeichnetes Produkt erfüllt grundlegende Cybersicherheitsanforderungen.

FOTO: AIT

Christoph Schmittner, MSc
Senior Scientist

Hersteller:innen und Betreiber:innen steht damit eine fundamentale Veränderung mit erheblichen Herausforderungen bevor. Hersteller:innen von Hard- und Software müssen Entwicklungsprozesse anpassen, Risiken systematisch bewerten, Schutzmechanismen von Anfang an in die Produktarchitektur integrieren und Sicherheit über die Lebenszeit des Produktes mitdenken. Noch komplexer wird es für Betreiber:innen von Anlagen. Diese arbeiten mit Systemen, die über Jahrzehnte im Einsatz sind und deren Komponenten oft über lange Zeiträume hinweg identisch nachbeschafft werden müssen.

Mit Inkrafttreten des CRA dürfen Hersteller:innen ab 12. Dezember 2027 jedoch keine nicht-konformen Produkte mehr auf den Markt bringen. Wer danach eine bestehende Anlage erweitern oder modernisieren will, steht vor einer Herausforderung. Denn: Verfügbare Produkte sind zwar CRA-konform, doch nicht zwingend mit Steuerungssystemen aus den 1990er- oder 2000er-Jahren kompatibel. In der IT mag es normal sein, auf die nächste Produktgeneration umzusteigen. Bei digitalen Steuerungssystemen im Energie-, Produktions- und Transportbereich ist das hingegen ein Projekt enormen Ausmaßes.

Die einzige nachhaltige Antwort auf diese Herausforderungen ist der Paradigmenwechsel in Richtung: Security by Design. Statt Sicherheit nachträglich einzubauen, wird sie von Anfang an mitgedacht. Security by Design ist keine abstrakte Forderung, sondern eine gesetzliche Pflicht: Der CRA verlangt, dass Sicherheit in allen Phasen des Produktlebenszyklus berücksichtigt wird.

Im Zentrum steht die systematische Risikoanalyse. Sie schafft Klarheit über Zweck, Umfeld, Daten und Nutzer:innen eines Produkts und bildet so die Basis, um Bedrohungen und Risiken zuverlässig zu identifizieren. Dieser Prozess umfasst:

- **Produktkontext:** Zweck, Funktionen, Einsatzumgebung, Architektur, Nutzer:innenprofile
- **Bedrohungsanalyse:** Angriffsszenarien und mögliche Auswirkungen
- **Bewertung & Behandlung:** Eintrittswahrscheinlichkeit, Schadenshöhe, Maßnahmen
- **Kommunikation & Review:** Transparente Darstellung und regelmäßige Aktualisierung.

Die Risikoanalyse legt fest, welche essenziellen Anforderungen des CRA tatsächlich relevant sind. Speichert ein Produkt beispielsweise keine personenbezogenen Daten, entfallen Vorgaben zur verschlüsselten Speicherung. Wird ein Produkt nur in geschützten Industrieanlagen betrieben, können Bedrohungen schon durch den Kontext ausgeschlossen sein. Umgekehrt gilt: Je offener die Umgebung und je sensibler die Daten sind, desto strenger sind auch die Anforderungen.

De facto gibt es jedoch selbst bei Schwachstellen Spielraum: Der CRA verbietet zwar, Produkte mit ausnutzbaren Schwachstellen auf den Markt zu bringen, doch „ausnutzbar“ ist nur, was ein:e Angreifer:in unter realen Bedingungen tatsächlich verwenden könnte. Ist ein Interface im vorgesehenen Kontext nicht zugänglich, kann die Schwachstelle als nicht ausnutzbar bewertet werden und muss nicht zwingend geschlossen werden.

Damit ist die Risikoanalyse die Basis für alle Anforderungen. Sie entscheidet, welche Maßnahmen verpflichtend sind und welche vertretbar weggelassen werden können, und dokumentiert diese Entscheidungen nachvollziehbar für Hersteller:innen, Betreiber:innen und Aufsichtsbehörden.

Damit Security by Design nicht Theorie bleibt, braucht es Werkzeuge, die den Prozess unterstützen. Ein Beispiel ist ThreatGet, entwickelt vom AIT Austrian Institute of Technology. ThreatGet ermöglicht modellbasierte Risiko- und Bedrohungsanalysen direkt auf Basis von Architekturmodellen. Risiken werden automatisiert erkannt, Sicherheitsanforderungen abgeleitet und die notwendige Dokumentation erstellt – ein entscheidender Vorteil angesichts der Nachweispflichten des CRA. Darüber hinaus zeigt ThreatGet, dass Europa nicht nur Regulierung vorgibt, sondern auch konkrete Lösungen entwickelt. Hersteller:innen und Betreiber:innen erhalten damit ein geeignetes Tool, um Security by Design effizient in ihre Prozesse einzubauen, unabhängig davon, ob es um vernetzte Konsumprodukte oder komplexe Industrieanlagen geht.

Der Cyber Resilience Act verändert die Spielregeln. Für Konsument:innen bedeutet er mehr Sicherheit, für Hersteller:innen und Betreiber:innen erhebliche Umstellungen. Doch wer Security by Design frühzeitig integriert, gewinnt mehr als nur regulatorische Konformität: Vertrauen wird zum Wettbewerbsvorteil. ■

Wer (Cyber-)Sicherheit nicht ernst nimmt, bekommt mit Sicherheit Probleme

Im Interview informiert der Geschäftsführer der Infotech EDV-Systeme GmbH, Martin Mallinger, zur Lage der Cybersecurity in österreichischen Unternehmen. Außerdem spricht er über häufige Herausforderungen und darüber, wie sich diese meistern lassen.

FOTO: INFOTECH EDV-SYSTEME GMBH

Ing. Martin Mallinger, MSc
Geschäftsführer

Wie cybersicher sind österreichische Unternehmen?
Große Unternehmen sind bei der Cybersecurity häufig weiter als KMUs, immer häufiger haben sie eigene Expert:innenteams. Oft sind Unternehmen schon mit grundlegenden Sicherheitsmaßnahmen überfordert (Patch Management, Backup, Benutzer:innenverwaltung und Multi-Faktor-Authentication, MFA). Das macht sie angreifbar.

Schätzen hiesige Unternehmer:innen digitale Souveränität?
Den meisten EU-Unternehmen ist ihre große Abhängigkeit von US-amerikanischen Unternehmen (noch) nicht bewusst. Zwänge die US-Regierung US-Unternehmen mit Sanktionen dazu, EU-Unternehmen den Zugriff auf ihre Cloud-Services zu verbieten, hätten viele EU-Unternehmen keinen Zugriff mehr auf E-Mails, Telefonie und Unternehmensdaten. Deshalb raten wir unseren Kund:innen, sich Gedanken über Exit- und Notfallszenarien zu machen, wenn sie cloudbasierte Services aus den USA nutzen. Als Anbieter souveräner Cloud-Services sichern wir Daten von Unternehmen in selbstbetriebenen, lokalen Clouds.

Wichtig: Für ein Mehr an Souveränität muss man nicht mit dem Schwierigsten, wie der Ablöse von MS-365-Services starten. Für viele einfache Anwendungen gibt es Alternativen – auch von regionalen Cloud-Anbietern, wie z. B. den my.bizcloud-Services (https://www.mybizcloud.at) aus unserem Haus.

Was sind die drei größten Schwachstellen von Unternehmen?
1. Ganz weit vorne ist die Annahme, dass das eigene Unternehmen für Angreifende uninteressant ist, weil es nichts zu holen gibt.
2. Es wird oft angenommen, dass IT-Sicherheit nur ein Kosten- und nicht auch ein Erfolgsfaktor ist.
3. Die steigende Komplexität der IT-Systemlandschaft ist schwer zu schützen.

Mit der NIS2-Richtlinie hat Europa eine EU-weite Vorgabe, um Cybersecurity zu schaffen. Ist das eine Herausforderung für Österreichs Unternehmen?
NIS2 ist vielen ein Begriff. Leider werden die Anforderungen meist negativ betrachtet, obwohl die Maßnahmen Unternehmen schützen und auf etablierten internationalen Standards (ISO/IEC 27001, 27002) beruhen. Zudem berücksichtigt NIS2 Größe und Möglichkeiten der Unternehmen. Das Besondere an der Entwicklung der nationalen Umsetzungen ist, dass viel Expert:innenwissen eingeflossen ist. Etwas unglücklich ist, dass es die letzte Regierung nicht geschafft hat, das Gesetz zu verabschieden. Das verwirrt und verunsichert Unternehmen. Viele bereits initiierte NIS2-Projekte liegen deshalb auf Eis.

Viele Unternehmen stecken noch zu viel Energie in Argumentation und Auswegsuche, um nicht unter NIS2 zu fallen – es gibt sogar Ideen zum Umstrukturieren der Gesellschaften. Davon ist klar abzuraten. Ihre Energie sollten Unternehmen lieber in eine vernünftige Umsetzung investieren.

Die größten Kritikpunkte an NIS2 sind die Feststellung der Betroffenheit (Fällt mein Unternehmen unter NIS2?) und die konzernweite/länderübergreifende Umsetzung.

Haben Sie ein Beispiel für die Umsetzung einer NIS2 Maßnahme?
Die NIS2 wird bei der Netzwerksegmentierung sehr konkret: Netze sind demnach gemäß der Risikobewertung funktional/logisch zu trennen und kritische Systeme in besonders gesicherten Zonen unterzubringen. Beide Schutzmaßnahmen sind seit Langem Best Practice – und werden dennoch von vielen Unternehmen nicht umgesetzt. Wir bieten hierfür mit unserem Partner Zero Networks moderne Lösungen an, die tatsächlich nicht nur Netzbereiche, sondern einzelne Geräte voneinander segmentieren können, und zwar auf automatisierte Art und Weise. Zudem ermöglichen wir, dass jede Verbindung, egal von welchem Nutzer, Anwendung, Protokoll oder Asset mit einer MFA (Multi Factor Authentication) versehen werden kann.

NIS2 fordert Unternehmen auch zur Notfallvorsorge auf: Kommen die Unternehmen dem nach?
Unternehmen müssen wissen, wie sich Ausfälle einzelner Systeme auf den Geschäftsbetrieb auswirken. Ein Großteil des Schadens lässt sich häufig mit einfachen Maßnahmen deutlich senken. Für verbleibende, nicht verhinderbare Ausfälle braucht es Notfallpläne. Und die sollten unbedingt auch geübt werden. Wir machen mit Kund:innen regelmäßig Disaster-Recovery-Tests. Die Testergebnisse dokumentieren wir, sodass sie als erster Notfallplan dienen können. Wichtig: Im Notfall müssen die Notfallpläne – unabhängig von den eigenen Systemen – verfügbar sein! ■

Lesen Sie mehr unter
infotech.at

Cybersecurity ist Chefsache: So schützen Sie Ihr Unternehmen einfach und zuverlässig.

Das Internet ist längst nicht mehr nur Kommunikationskanal oder Vertriebsweg – es ist die Lebensader moderner Unternehmen. Doch wer online sichtbar ist, ist auch angreifbar: Cyberattacken, Ausfälle und digitale Manipulationen gehören heute zu den größten Geschäftsrisiken. Wie lässt sich ein Unternehmen schützen, ohne selbst IT-Experte zu sein?
Die Antwort lautet nic.at. Als Registrierungsstelle für .at-Domains steht nic.at seit fast 30 Jahren für Stabilität und digitale Souveränität. Gemeinsam mit den Dienstleistungen ihrer Schwester- und Tochterfirmen – RcodeZero DNS, CERT.at und tldbox – bildet nic.at ein einzigartiges Kompetenzzentrum für Internetsicherheit. Von der Domainverwaltung bis hin zu spezialisierten Sicherheitslösungen erhalten Unternehmen alles aus einer Hand. 100 % Internetkompetenz aus Österreich, für eine digitale Zukunft, auf die Sie bauen können.

Die eigene Domain – Mehr als nur ein Name

Eine eigene Domain ist wie ein Stück Land in der digitalen Welt: Sie bringt Rechte und Pflichten, eröffnet aber vor allem Chancen, im Internet sichtbar zu sein und gefunden zu werden. Die beiden Geschäftsführer von nic.at, Andreas Musielak und Robert Schischka, erklären im Interview, warum eine Domain so wichtig ist und worauf Unternehmen achten sollten.

FOTO: NIC.AT

Robert Schischka
technischer Geschäftsführer bei nic.at

FOTO: NIC.AT

Andreas Musielak
kaufmännischer Geschäftsführer bei nic.at

Was ist die Aufgabe von nic.at?
Robert Schischka (RSCH): Unsere Hauptaufgabe ist die Vergabe und Verwaltung von .at-Domainnamen. Man kann sich das wie ein digitales Grundbuch vorstellen: Jede Domain wird weltweit nur einmal vergeben, damit es keine Doppelungen gibt. Doch wir sind weit mehr als eine Datenbank. Im Hintergrund sorgen wir dafür, dass die technischen Abläufe zuverlässig funktionieren – damit Webseiten und E-Mails mit einer .at-Domain jederzeit erreichbar sind.

Wie kann eine eigene Domain registriert werden?
Andreas Musielak (AM): Auf unserer Webseite www.nic.at können Interessierte prüfen, ob der gewünschte Domainname verfügbar ist. Falls dieser bereits vergeben ist, zeigen wir freie Alternativen an.

RSCH: In der Praxis läuft die Registrierung meist über sogenannte Registrare oder Provider. Dort erhält man nicht nur die Domain, sondern ein ganzes Servicepaket rund um die eigene Online-Präsenz: von der Webseite, über E-Mail-Adresse bis hin zum Hosting. Die Domain ist also der erste Baustein für den gesamten Internetauftritt.

Warum ist ein Domainname so wichtig?
AM: Der Domainname ist das digitale Aushängeschild eines Unternehmens. Trotzdem starten viele Gründer:innen, ohne vorher zu prüfen, ob ihre Wunschdomain noch frei ist und müssen später umständliche Kompromisse eingehen, indem sie mit kreativen Lösungen versuchen, den Namen irgendwie hinzubekommen. Dabei begleitet eine Domain das Unternehmen oft für immer und prägt, wie Produkte oder Dienstleistungen online präsentiert werden.

Eine Domain kann zwar jederzeit gelöscht werden, doch dieser Schritt sollte gut überlegt sein: Nach einer Frist wird sie wieder frei und kann von jeder beliebigen Person neu registriert werden. Ab diesem Zeitpunkt hat der/die ursprüngliche Inhaber:in keine Kontrolle mehr darüber, welche Inhalte dort erscheinen.

RSCH: Wir sehen häufig, dass Unternehmen oder auch Politiker:innen Kampagnen starten und dann überrascht feststellen, dass die passende Domain längst vergeben ist. Zwischenzeitlich galt es zudem als Trend, Webseiten durch reine Social-Media-Präsenz zu ersetzen. Aber es ist meinem Empfinden nach schnell Ernüchterung eingetreten, denn Plattformen können ihre Regeln jederzeit ändern und so Reichweite oder Inhalte beeinflussen. Mit einer eigenen Domain schafft man sich dagegen Unabhängigkeit und Verlässlichkeit. Das Prinzip ist dabei einfach: first come, first served. Wer eine Domain zuerst registriert, hat die Rechte daran – solange keine Marken- oder Namensrechte verletzt werden.

Lesen Sie mehr unter
www.nic.at

Was sollte im Vorfeld einer Registrierung beachtet werden?
RSCH: Wichtig ist, die Eigentumsverhältnisse von Anfang an klar zu regeln. Ein Beispiel: Drei Freunde gründen ein Unternehmen und registrieren gemeinsam eine Domain. Jahre später trennen sie sich im Streit und plötzlich ist unklar, wem die Domain gehört. Gerade wenn die Domain für die Kundenkommunikation zentral ist, braucht es klare Vereinbarungen. Viele Konflikte ließen sich vermeiden, wenn man das gleich zu Beginn festlegt. Eine Domain ist ein wertvolles Asset – vergleichbar mit einem Investment in ein physisches Produkt oder einen neuen Standort.

AM: Als Vergabestelle beurteilen wir keine Inhalte von Webseiten. Bei offensichtlichen Marken- oder Namensrechtsverletzungen können wir jedoch auf eine etablierte Rechtsprechung zurückgreifen und so wirksam einschreiten. Genau diese gefestigte Rechtslage ist ein weiterer wesentlicher Vorteil einer .at-Domain gegenüber anderen Domain-Endungen oder einer Social-Media-Präsenz.

Ein letzter Tipp?
AM: Bei der großen Auswahl an Domain-Endungen liegt man mit einer .at-Domain immer richtig. Studien zeigen: Über 96 % der Österreicher:innen verbinden .at mit Sympathie, Vertrauen, Sicherheit und Regionalität – ein klares Signal für alle, die in Österreich online sichtbar und glaubwürdig auftreten wollen. ■

.AT – DAS ZUHAUSE IM INTERNET DER ÖSTERREICHER:INNEN

Weltweit gibt es rund 372 Millionen registrierte Domains – verteilt auf über 1.400 Domain-Endungen. Die bekannteste ist .com, doch für Österreich hat sich .at als klare Nummer eins etabliert: Mehr als 1,4 Millionen .at-Domains sind registriert, knapp drei Viertel davon auf Inhaber:innen mit österreichischer Postadresse. nic.at ist seit 1998 die offizielle Vergabestelle für .at-Domains. Sie sorgt dafür, dass jede .at-Domain eindeutig, sicher und weltweit erreichbar ist. **www.nic.at**

RcodeZero DNS

DNS als DNA der Cybersicherheit

Cyberangriffe in Form von DDoS-Attacken sind eine ernstzunehmende Gefahr für Unternehmen – vor allem dann, wenn der DNS-Server ins Visier genommen wird. Klaus Darilion, DNS-Experte und Head of Operations bei nic.at, spricht im Interview über diesen unscheinbaren, aber essenziellen Dienst und erklärt, wie sich Unternehmen wirksam absichern können.

FOTO: NIC.AT

Klaus Darilion
DNS Experte und Leiter Operations bei nic.at

Viele Unternehmen haben die DNS-Infrastruktur nicht unbedingt als erstes im Blick, wenn es um Cybersicherheit geht. Warum sollte man ihr dennoch besondere Beachtung schenken?
Das Domain Name System ist einer der grundlegendsten Dienste des Internets – ohne DNS läuft nichts. Es übersetzt Domainnamen wie example.com in IP-Adressen, sodass Computer miteinander kommunizieren können. Fällt das DNS aus, können weder Webseiten aufgerufen, noch E-Mails verschickt oder ERP-Systeme genutzt werden. Im schlimmsten Fall kommt die gesamte digitale Kommunikation eines Unternehmens zum Stillstand. Obwohl das DNS so zentral ist, wurde es in der Vergangenheit oft übersehen oder stiefmütterlich behandelt. Genau das macht es heute zu einem attraktiven Ziel für Angreifer:innen.

Welche Gefahren sind dabei besonders relevant?
Wir sehen eine massive Zunahme von DDoS-Angriffen. Laut dem European Cyber Report 2025 haben sich diese im Vergleich zum Vorjahr mehr als verdoppelt. Die Bandbreiten erreichen Rekordwerte von über 1,4 Terabit pro Sekunde. Dabei muss man unterscheiden: Volumetrische Attacken überlasten die Internetverbindung durch enormes Datenaufkommen und legen so ganze Leitungen lahm. Gegen diesen Typ sind viele Unternehmen bereits mit klassischen DDoS-Mitigation-Systemen abgesichert. Die zweite Kategorie sind zielgerichtete Angriffe auf das DNS selbst. Diese treffen direkt den autoritativen Nameserver. Fällt dieser aus, stehen binnen Sekunden zentrale Geschäftsprozesse still – mit gravierenden Folgen wie Umsatzeinbußen, Produktionsausfällen und Reputationsschäden. Genau gegen diese Angriffe sollten Unternehmen mit DNS-Profis sprechen oder spezialisierte Services wie unseren in Anspruch nehmen.

Viele Firmen setzen beim Schutz auf ihre zentrale Firewall. Warum reicht das nicht aus?
Weil DNS-Server öffentlich erreichbar sein müssen. Eine Firewall ist wichtig, aber zum Schutz des DNS ist sie nicht geeignet. Angreifer:innen überlasten die Firewall mit sinnlosen Anfragen. Das Problem: Nicht nur der DNS-Server fällt aus, sondern oft gleich das gesamte Unternehmensnetzwerk. Das ist, als würden plötzlich tausende Kund:innen gleichzeitig durch die Eingangstür eines Geschäfts stürmen – am Ende kommt niemand mehr durch. Die bessere Lösung ist, Nameserver getrennt von der zentralen Firewall zu betreiben und diese mit speziellen Schutzmechanismen abzusichern, die nur auf DNS-Anfragen reagieren. So bleibt die übrige Infrastruktur auch bei Angriffen stabil.

Wie kann ein Unternehmen seine DNS-Infrastruktur resilient machen?
Es gibt drei wesentliche Prinzipien, um möglichst gut aufgestellt zu sein:

1. Redundanz schaffen: Mehrere autoritative Name-Server an unterschiedlichen Standorten. Fällt einer aus, übernehmen die anderen und die Dienste bleiben erreichbar.
2. Multi-Provider einsetzen: Nie

Lesen Sie mehr unter
www.rcodezero.at

nur auf einen Anbieter verlassen. Das DNS unterstützt den Betrieb mehrerer Provider ohne großen Aufwand. So verteilt man das Risiko und erhöht die Ausfallsicherheit.

3. Split-DNS nutzen: Öffentliche Anfragen werden von externen Servern beantwortet, interne Anfragen von internen Servern. Damit bleibt die interne Kommunikation auch dann bestehen, wenn es Angriffe von außen gibt.

Viele Unternehmen fragen sich: DNS selbst betreiben oder lieber outsourcen?
Das hängt stark von den Ressourcen und Kompetenzen in der IT-Abteilung ab. Eigener Betrieb bedeutet: ständige Wartung, Updates, Monitoring und Reaktionsbereitschaft rund um die Uhr. Das ist aufwendig und bindet enorme Ressourcen. Daher lohnt sich für die meisten Unternehmen Outsourcing an spezialisierte Provider. Professionelle Anbieter betreiben hochverfügbare, weltweit verteilte Netze, kümmern sich um Updates, liefern Statistiken und bieten Support rund um die Uhr. In Österreich sind wir mit RcodeZero DNS in dieser Form der einzige Anbieter. Unsere Premium-Variante bietet zudem detaillierte Analysen, die wertvolle Einblicke in die Nutzung und mögliche Angriffsmuster geben sowie einen persönlichen 24/7-Support.

Verglichen mit den potenziellen Schäden durch einen Angriff sind die Kosten für professionelle DNS-Dienste sehr gering. Wichtig ist, auf ein transparentes Modell zu achten. Manche Anbieter rechnen pro DNS-Anfrage ab – bei einem DDoS-Angriff explodieren die Kosten dann regelrecht. Wir setzen deshalb auf ein Flat-Fee-Modell: Unternehmen zahlen einen fixen Betrag und haben volle Planungssicherheit, egal wie viele Anfragen verarbeitet werden.

Welche Rolle spielt die neue europäische NIS2-Richtlinie dabei?
Mit NIS2 wurde DNS als kritische Infrastruktur eingestuft und gilt somit als besonders schützenswert. Das bedeutet, strengere Sicherheitsanforderungen und Compliance-Vorgaben für Betreiber:innen. Wir sind nach ISO 27001 zertifiziert und erfüllen bereits seit 2014 viele Vorgaben, die durch NIS2 verbindlich geworden sind. Unternehmen, die ihre DNS-Dienste an zertifizierte Anbieter wie uns auslagern, können damit einzelne Anforderungen von NIS2 abdecken und sparen sich Aufwand bei der Umsetzung.

Was raten Sie Entscheidungsträger:innen konkret?
Mein wichtigster Rat: Warten Sie nicht, bis ein Angriff passiert. Vorausschauende Planung ist entscheidend. Gerade in ruhigen Zeiten sollten Unternehmen ihre Cybersecurity-Maßnahmen überprüfen und ihre DNS-Infrastruktur kritisch hinterfragen. Eine moderne DNS-Architektur mit Redundanz, Multi-Provider-Strategie und klarer Trennung von internen und externen Servern kostet im Verhältnis wenig, schafft aber enorme Sicherheit. ■

CERT.at

Das „unsichtbare“ Einsatzteam für Österreichs digitale Sicherheit

Cyberangriffe treffen längst nicht mehr nur internationale Konzerne. Auch österreichische Unternehmen, vom kleinen Handwerksbetrieb bis zum Industriekonzern, sind ein beliebtes Ziel. Doch wer hilft im Ernstfall? Wolfgang Rosenkranz, Teamleiter des nationalen Computer Emergency Response Teams, erklärt im Interview, wie CERT.at arbeitet, warum Eigenverantwortung entscheidend ist und welche Schritte jedes Unternehmen setzen sollte, um digital sicherer zu werden.

Was genau ist das CERT.at und welche Rolle spielt es in Österreich?
CERT.at ist das nationale Computer Emergency Response Team Österreichs. Also die zentrale österreichische Anlaufstelle rund um IT-Sicherheit. Wir unterstützen und koordinieren bei Cyberangriffen, wir vernetzen Sicherheitsexpert:innen untereinander – mit Behörden sowie internationalen Organisationen – und wir geben Warnungen und Tipps speziell auch für kleine und

FOTO: ANNA RAUCHENBERGER

Wolfgang Rosenkranz
Teamleiter CERT.at

mittlere Unternehmen heraus, die beschreiben, wie sie sich vor Angriffen schützen können. Unsere tägliche Aufgabe ist es, den Angreifer:innen einen Strich durch die Rechnung zu machen, indem wir Österreich schneller sicher machen, als sie uns attackieren können.

Wie informieren Sie Unternehmen über aktuelle Gefahren?

Wir sind keine klassische Nachrichtenorganisation, die täglich Schlagzeilen produziert. Das machen schon viele andere. Stattdessen prüfen unsere Spezialist:innen täglich eine enorme Menge an Informationen, filtern diese und geben nur das weiter, was für österreichische Organisationen relevant ist und wo Handlungsbedarf besteht. Auf unserer Webseite veröffentlichen wir beispielsweise Hintergrundinformationen zu kritischen Sicherheitslücken und Bedrohungen. Bei akuten Risiken versenden wir gezielte Warnungen an jene Gruppen, die betroffen sein können. Und wenn wir feststellen, dass eine Organisation direkt angegriffen wird, nehmen wir persönlich Kontakt auf. Unser Grundsatz lautet: Wir melden uns nur, wenn nötig. Aber wenn wir uns melden, dann ist es wichtig und sollte ernst genommen werden.

Können Sie uns Einblicke in Ihre tägliche Arbeit geben?

Wir analysieren täglich zehntausende Datensätze, die Hinweise auf verdächtige Aktivitäten enthalten könnten. Mit speziell entwickelter Software stellen wir fest, wer diese Daten benötigt und informieren betroffene Unternehmen über deren Internetprovider oder direkt, wenn wir wissen, wer sie sind. Dahinter stecken viel Arbeit durch ein erfahrenes Team, komplexe Softwarelösungen und hohe Wartungskosten. Wichtig ist zu betonen, dass wir nicht aus kommerziellem Interesse handeln, sondern auf gesetzlicher Grundlage und zum Gemeinwohl Österreichs.

Cybersecurity und Cyberresilienz – wo liegt der Unterschied?

Cybersecurity bedeutet in erster Linie Schutz digitaler Systeme durch Firewalls, Virenscanner oder Zugriffsrechte, die Angriffe verhindern sollen. Cyberresilienz geht einen Schritt weiter. Hier geht es um die Widerstandsfähigkeit, also darum, wie schnell ein Unternehmen nach einem Angriff wieder in so etwas wie einen Normalbetrieb zurückkehren kann. Ein Beispiel: Wenn Ihr Unternehmen Opfer einer Ransomware-Attacke wird, ist es entscheidend, ob Sie aktuelle Backups haben. Mit Backups können Sie in der Regel Ihre Systeme relativ rasch wiederherstellen, ohne im schlimmsten Fall alles neu aufbauen zu müssen.

Es muss uns allen bewusst sein, dass Cybersecurity und Cyberresilienz zentrale Erfolgsfaktoren der digitalen Welt sind. Digitale Sicherheit beginnt dabei immer mit Eigenverantwortung: Jedes Unternehmen muss den Grundschutz seiner Systeme selbst sicherstellen, etwa durch regelmäßige Datensicherungen, aktuelle Virenschutzprogramme und konsequente Updates. CERT.at und andere externe Stellen können unterstützen, doch die Basismaßnahmen müssen im Unternehmen selbst verankert und ernst genommen werden.

Wie können Unternehmen Angriffe erkennen?

Das ist oft nicht einfach. Viele Angriffe sind so konzipiert, dass sie möglichst lange unentdeckt bleiben. Grundsätzlich gilt: Nur wer aktiv sucht, findet auch etwas. Und hier kommt die gute Nachricht: Das funktioniert im ersten Schritt bereits gut, wenn ein Virenscanner im Hintergrund läuft – den gibt es in jedem modernen Betriebssystem oder man kauft sich ein Produkt seiner Wahl. Wichtig ist aber, dass dieser aktuell ist und dass man ihn auch aktiv nach Schadsoftware suchen lässt. Darüber hinaus braucht es weitere Investitionen in Sicherheit, sei es durch professionelle IT-Betreuung, Monitoring oder regelmäßige Updates. Cybersecurity ist kein „Gratisprodukt". So wie Sie in Brandschutz oder Versicherung investieren, müssen Sie auch die digitale Sicherheit als fixen Kostenfaktor einplanen.

Wie wichtig ist internationale Zusammenarbeit in diesem Bereich?

Sehr wichtig! Cyberangriffe machen nicht an Landesgrenzen halt. Über die europäische NIS-Richtlinie haben wir einen gesetzlichen Auftrag und sind weltweit mit Partnerorganisationen vernetzt. In diesem Netzwerk tauschen wir Informationen aus und können im besten Fall schneller reagieren als die Angreifer:innen. Gelingt das nicht, verhindern wir zumindest, dass der Schaden auf andere Unternehmen übergreift. CERT.at arbeitet damit als Teil eines nationalen und globalen Sicherheitsnetzes. Wir sorgen gemeinsam dafür, dass die digitale Infrastruktur, die wir alle selbstverständlich nutzen – vom Online-Banking bis zur Produktionssteuerung – stabil und sicher bleibt.

Was ist Ihre wichtigste Empfehlung für Unternehmen?

Sehen Sie digitale Sicherheit als Chefsache, genauso wie Finanzen oder Personal. Nehmen Sie Warnungen von CERT.at ernst, investieren Sie in Grundschutz und bereiten Sie sich aktiv auf Zwischenfälle vor. Denn eines ist sicher: Wer vorbereitet ist, kann Angriffe nicht nur besser abwehren, sondern auch Betriebsunterbrechungen so kurz wie möglich halten und die gewohnten Abläufe rasch wiederherstellen. ■

Lesen Sie mehr unter
www.cert.at

ÜBER CERT.AT

CERT.at ist das nationale Computer Emergency Response Team Österreichs. Es koordiniert die Reaktion auf IT-Sicherheitsvorfälle, unterstützt Unternehmen und Organisationen bei der Abwehr von Angriffen und gibt Warnungen sowie praxisnahe Tipps weiter. Auf der Webseite **www.cert.at** können sich Interessierte in Mailinglisten eintragen, um regelmäßig Warnungen zu aktuellen IT-Sicherheitsproblemen sowie ausgewählte Links aus der täglichen Quellenbeobachtung zu erhalten. Außerdem besteht die Möglichkeit, direkt über **www.cert.at** Sicherheitsvorfälle zu melden.

tldbox

Eine eigene Top-Level-Domain: Gütesiegel und Marketinginstrument

Nach 13 Jahren bietet die Internetorganisation ICANN (Internet Corporation for Assigned Names and Numbers) im Frühjahr 2026 wieder die Möglichkeit, sich für eine Top-Level-Domain zu bewerben. Über den Ablauf und die Vorteile spricht Fritz Diekmann, Business Development Manager bei tldbox, einem Service von nic.at.

Welchen Vorteil hat eine Top-Level-Domain (TLD)?
Eine TLD ist die Endung einer Internetadresse. Bekannte Beispiele sind .at für Österreich oder .com für commercial. Seit 2012 gibt es zusätzlich neue Endungen mit allgemeinen Begriffen wie .club, Städtenamen wie .tokyo oder Markennamen wie .bmw. Eine Domain-Endung ist mehr als technisches Detail. Sie schafft Identität sowie Sicherheit in der Nutzung durch eigene Vergaberichtlinien.

Die TLD ist außerdem digitales Gütesiegel und wirkungsvolles Marketinginstrument. Statt firma.com könnte die Adresse firma.marke oder firma.region lauten. Das ist ein digitales Aushängeschild, das Vertrauen schafft und einen starken Wiedererkennungswert hat.

Als Markeninhaber:in kontrollieren Sie alle Domains selbst und stellen sicher, dass niemand Ihre Produktnamen oder Markenbegriffe blockieren oder missbrauchen kann. Gerade weil die Zahl der Domain-Endungen wächst und die Komplexität im Markenschutz steigt, bietet eine TLD für globale Unternehmen eine attraktive Lösung. Spannend ist eine TLD auch für Akteure mit regionalem Bezug, z. B. Tourismusbetriebe oder regionale KMU. Das Erfolgsbeispiel .wien zeigt, wie viel Potenzial besteht.

Wie kompliziert ist der Bewerbungsprozess?
Das Bewerbungsverfahren bei ICANN ist streng geregelt. Bewerber:innen müssen sich an ein Handbuch halten sowie ein Geschäftsmodell, technische Konzepte und Nachweise über die langfristige Tragfähigkeit vorlegen. Genau hier kommen wir ins Spiel: Bereits 2012 haben wir zahlreiche Bewerbungen wie .berlin erfolgreich begleitet. Wir führen Interessent:innen durch den komplexen Gesamtprozess. Der Start der neuen Bewerbungsrunde ist für Frühjahr 2026 geplant. Das Bewerbungsfenster ist voraussichtlich bis Juli/August 2026 geöffnet. Wir rechnen mit großem Interesse: Schon 2012 gab es 1.930 Bewerbungen, aus denen ca. 1.200 neue Domain-Endungen hervorgingen.

Wie unterstützen Sie interessierte Unternehmen?
Wir begleiten Unternehmen auf dem gesamten Weg zur TLD. Gemeinsam mit unserer Schwesterfirma nic.at haben wir über 37 Jahre Expertise in Verwaltung und Betrieb von Domain-Endungen. Höchste Standards in Sicherheit, Stabilität und Datenschutz sind durch ISO 27001, DSGVO- und NIS2-Konformität garantiert. Dank der engen Zusammenarbeit mit CERT.at sind wir auch bei Cybersecurity auf dem neuesten Stand. Zusätzlich bieten wir leistungsfähige Systeme, die global 24/7 verfügbar sind.

Ab wann und wie lange ist eine TLD gültig?
Mit dem Zuschlag für die TLD entsteht ein Vertrag mit ICANN, der grundsätzlich dauerhaft gilt. Wichtig ist: Marken- und Namensrechte bleiben stets geschützt. Nach der Zuteilung dauert es bis zu 24 Monate, bis die neue Domain-Endung technisch eingeführt und in die Root-Server eingetragen ist.

Haben Sie Tipps für Unternehmen?
Für eine Bewerbung sollte man ca. ein halbes Jahr Vorbereitung einplanen. Je früher Sie beginnen, desto besser lassen sich Geschäftsmodelle entwickeln und Strukturen aufbauen. Da der Prozess viel Zeit und (finanzielle) Ressourcen erfordert, gilt: Wer rechtzeitig plant, steigert nicht nur die Erfolgsaussichten auf die eigene digitale Marke, sondern senkt auch die Kosten. ■

Interessierten bieten wir am 21. Oktober 2025 um 11 Uhr ein kostenloses Webinar an, Anmeldung unter www.tldbox.at.

FOTO: NIC.AT

Fritz Diekmann
Business Development Manager

Lesen Sie mehr unter
www.tldbox.at

TLDBOX – IHR PARTNER FÜR TOP-LEVEL-DOMAINS

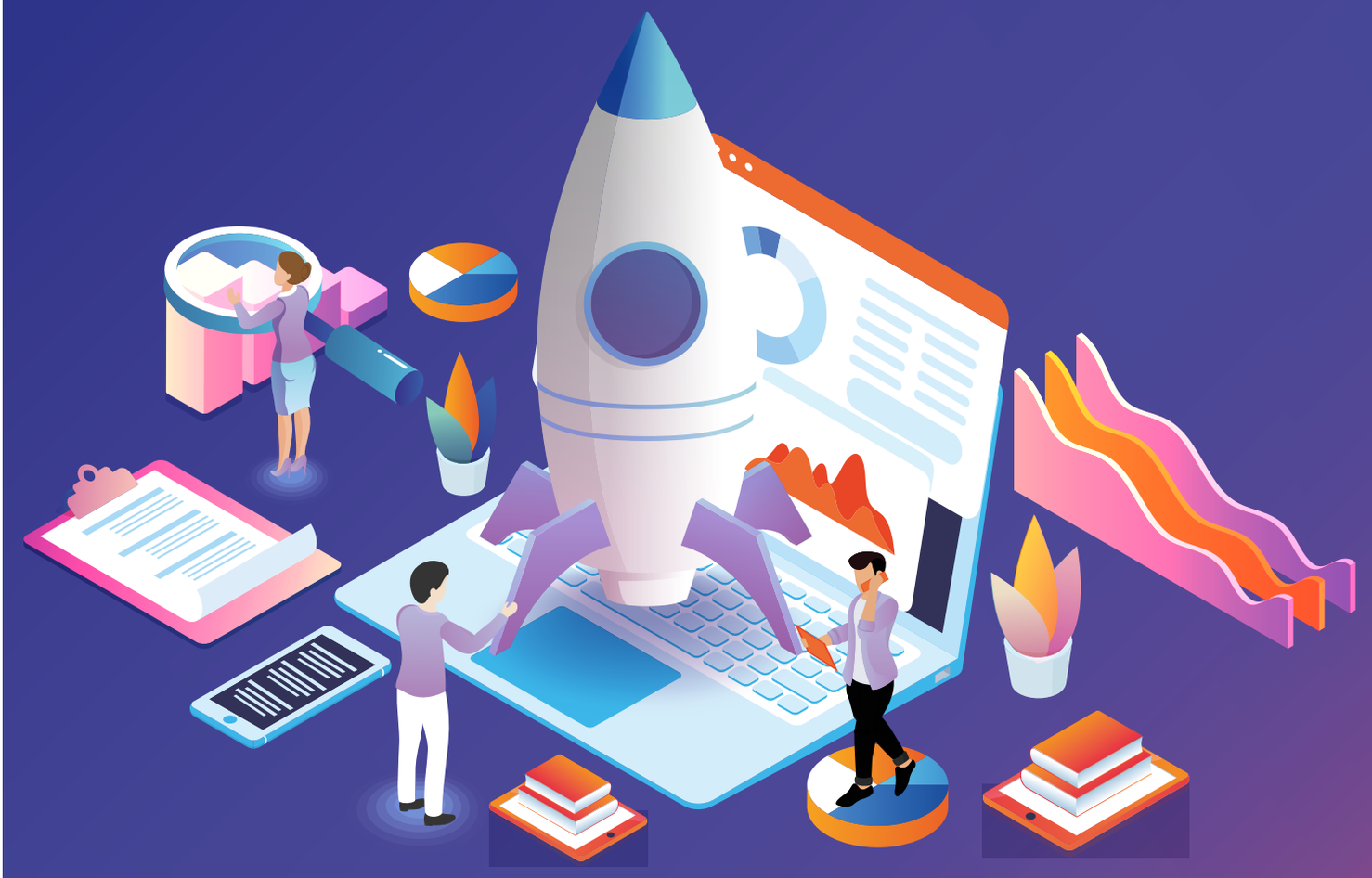
Mit über 37 Jahren Erfahrung aus dem Betrieb von .at durch unsere Schwesterfirma nic.at vereinen wir höchste Sicherheit und technologische Spitzenleistung mit persönlicher Betreuung und Verlässlichkeit. Von der Bewerbung bis zum laufenden Betrieb bieten wir alles aus einer Hand, transparent, flexibel und auf Augenhöhe. Unsere Systeme sind weltweit verfügbar, ISO-zertifiziert und stabil im Einsatz. So machen wir Ihre digitale Identität sichtbar, vertrauenswürdig und zukunftssicher, **www.tldbox.at**.

Werden Sie Opinion Leader in Ihrer Branche!

mediaplanet

HoliSec

Holistic Cyber Security



Sind Ihre Daten wirklich sicher? Finden wir es heraus.

- Security Quick Check: in nur 30 Minuten wissen, wo Ihr Unternehmen steht
- Klare Roadmap: einfache Schritte statt teurer Großprojekte
- Wir bringen Wissen in Ihr Unternehmen: praxisnah & verständlich
- Richtig statt teuer: Cyber Security, die wirkt und leistbar bleibt

Bereit, Ihr Unternehmen in Sachen IT & Cybersicherheit auf das nächste Level zu bringen?

Scannen Sie den QR-Code für mehr Infos

HoliSec GmbH
Mariahilfer Straße 1
8020 Graz

+43 650 9940380

hello@holisec.com