www.ehzaustria.at

EHZ austria

Ihr Partner für den IKT-Handel

08 2025

BEDROHTE WELT

ZWISCHEN RISIKO UND RESILIENZ. Cyberangriffe werden komplexer, KI verändert die Abwehr, Lieferketten werden zur Schwachstelle. Security ist längst ein strategischer Dauerprozess.

CHANNEL-TALK
„Als europäischer Hersteller können wir zudem garantieren, dass unsere Produkte keine Backdoors enthalten.“
Seite 10
Matthias Malcher, Eset

AS media | Lautensackgasse 29/11, 1140 Wien
P.b.b. Österreichische Post AG – MZ 24Z044575 M

KEIN WINDOWS 11 PC UNTER DEM WEIHNACHTSBAUM?

KEIN PROBLEM!

Manchmal kommts ganz plötzlich:
Windows 10 hat am 14. Oktober das Ende des regulären Supports erreicht. Nicht alle Endkunden sind schon bereit für den Umstieg auf neue Hardware oder Windows 11. Zudem haben nicht alle Fachhändler ausreichend freie Kapazitäten, um den Umstieg zu bewältigen. Damit der Betrieb sicher weiterläuft, gibt es die Extended Security Updates (ESU) für Windows 10 zu besonders attraktiven Konditionen.

Mit den ESU erhalten Ihre Kunden weiterhin wichtige Sicherheitsupdates für Windows 10 – und gewinnen damit Zeit, ihre Umstellung auf neue Geräte oder Windows 11 strategisch zu planen.
Gleichzeitig entlastet das Ihre Techniker und sorgt für weniger Druck in der Migrationsphase.

Microsoft 365

WORTMANN AG empfiehlt Windows 11 Pro für Unternehmen.

ESU-AKTION: JETZT HANDELN LOHNT SICH DOPPELT!

50-100% GUTSCHRIFT SICHERN!

Wer jetzt die ESU für Windows 10 über unser TERRA CLOUD Center bucht, kann die Aktion aktiv nutzen:
Beim späteren Kauf eines Windows 11 Pro Gerätes mit Intel CPU gibt es:

- **50 % Gutschrift** auf den ESU-Preis
- **100 % Gutschrift** auf den ESU-Preis, wenn es sich um ein Copilot+ Gerät handelt!

So profitieren Sie gleich doppelt – von weiteren Sicherheitsupdates jetzt und von einer planbaren Umstellung im nächsten Jahr.

So funktioniert´s

1. Buchen Sie die ESU für Windows 10 im TERRA CLOUD Center unter www.terracloud.de.
2. Fügen Sie den Promoartikel in gleicher Menge zur Bestellung hinzu – damit wir wissen, dass Sie an der Aktion teilnehmen.
3. Beim späteren Kauf eines Windows 11 Pro oder Copilot+ Geräts geben Sie einfach die ursprüngliche ESU-Buchung an – die Gutschrift erfolgt durch Ihren Ansprechpartner im Vertrieb.

Die Aktion gilt ab sofort und bis auf Widerruf.
Gutschriften können **ab dem 01. Januar 2026 bis zum 31. Dezember 2026** beim Kauf eines Windows 11 Pro Gerätes mit Intel CPU eingelöst werden. Sie erhalten pro Gerät eine Gutschrift über 50% bzw. 100% der Kosten einer ESU-Lizenz.

Promo-Tipp: unser leistungsstarkes Copilot+ PC Notebook mit vorinstalliertem Windows 11 Pro!

Windows 11

TERRA MOBILE 1671L Ultra

- Intel® Core™ Ultra 5 Prozessor 228V (8 M Cache, bis zu 4,50 GHz)
- Windows 11 Pro
- Displaygröße 40.64 cm (16")
- 2560x1600 Pixel Display-Auflösung
- Display-Typ Non Glare
- 32 GB Speicherkapazität
- Intel® Arc™ 130V
- 1 TB Gesamtspeicherkapazität

Artikelnr.: 1220867

intel.

zum Produkt

WORTMANN AG Zweigniederlassung Österreich
Hirschstettnerstraße 19-21_1220 Wien
Telefon: +43 1.2020909-0_Telefax: +43 1.2020909-15
E-Mail: oesterreich@wortmann.de

www.wortmann.de

WORTMANN AG
IT. MADE IN GERMANY.

© Wolfgang R. Fürst

Mag. Barbara Sawka
Chefredakteurin

Liebe Leserinnen und Leser,

„Beim Reden kommen die Leut' zsamm", sagt man, und genau das spürt man auch in unseren Interviews: Wenn Expertinnen und Experten erzählen. Aus diesen Gesprächen entstehen nicht nur spannende Einblicke, sondern oft auch neue Perspektiven. Vier starke Interviews zeigen diesmal, wie vielfältig die Welt der IT ist: kluge Gedanken, ehrliche Antworten und echte Begeisterung für Technik und Menschen, die sie gestalten. Mir gefällt das!

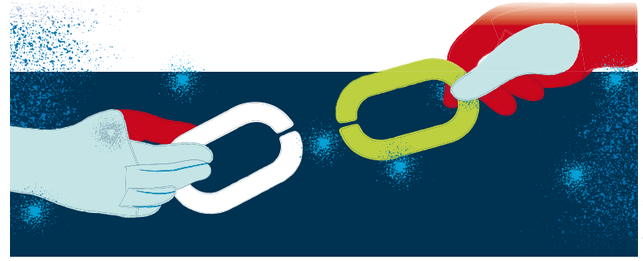
Oft merken wir erst, wie wichtig Security ist, wenn unsere Sicherheit bedroht ist. Vielleicht liegt darin auch ihre größte Herausforderung: Sie ist kein Zustand, sondern ein Prozess, der ständige Aufmerksamkeit verlangt. In dieser Ausgabe gibt es dazu einen kleinen Fokus.

Ich wünsche Ihnen viel Vergnügen beim Lesen,

Ihre Barbara Sawka

INHALT
NOVEMBER 2025

BRANCHE



© freepik

CHANNEL

TECHNIK

INDEX

Bundesheer

Kooperation für mehr Cybersicherheit

Mit einer Kooperation zwischen dem Bundesheer und dem Haus der Digitalisierung sollen künftig Wissen und Ressourcen gebündelt werden, um Österreichs digitale Verteidigungsfähigkeit weiter zu stärken. Besonders der fachliche Austausch an Informationen soll mittels Workshops, Seminaren, sowie gemeinsamen Forschungsprojekten intensiviert werden. Informationsoffiziere werden künftig an Schulen sowie bei öffentlichen Veranstaltungen über digitale Risiken und Sicherheitsthemen informieren. Zudem kann das Bundesheer die Räumlichkeiten vom Haus der Digitalisierung für Cyber-Übungen, Schulungen und Veranstaltungen nutzen.

© HBF/Carina Karlovits

Verteidigungsministerin **Klaudia Tanner,** Landeshauptfrau **Johanna Mikl-Leitner,** Generalsekretär BMLV **Arnold Kammel** und Geschäftsführer **Lukas Reutterer** bei der Unterzeichnung der Kooperationsvereinbarung.

Erste gemeinsame Schritte sind bereits geplant: Mit einer landesweiten „Roadshow 2026" sollen Schüler:innen und Eltern für Manipulationen im digitalen Raum sowie Cybersicherheit sensibilisiert werden. Im Dezember 2025 gibt es eine Schulung für Führungskräfte kritischer Infrastrukturen in Zusammenarbeit mit Fachstellen der NATO. Zusätzlich ist eine Informationsveranstaltung für KMU vorgesehen, bei der praxisnahe Einblicke in aktuelle Bedrohungslagen und Schutzmaßnahmen vermittelt werden.

www.bundesheer.at

© Freepik

TÜV Austria Group

NEUE REGELN

Ab 2027 gelten mit der EU-Maschinenverordnung und dem Cyber Resilience Act strenge Sicherheitsvorgaben für Hersteller. TÜV Austria und clockworkX unterstützen mit einer praxisnahen CSMS Masterclass.

Mit der neuen EU-Maschinenverordnung und dem Cyber Resilience Act (CRA) kommen ab 2027 verbindliche gesetzliche Anforderungen auf Hersteller von Maschinen und digitalen Produkten zu. Beide Regelwerke verfolgen das Ziel, die Sicherheit im europäischen Binnenmarkt zu erhöhen, setzen jedoch unterschiedliche Schwerpunkte. Die EU-Maschinenverordnung konzentriert sich auf die mechanische, elektrische und funktionale Sicherheit von Maschinen sowie sicherheitsrelevante Komponenten. Erstmals werden auch digitale Risiken berücksichtigt, etwa durch KI oder die Zusammenarbeit von Mensch und Roboter. Hersteller sind verpflichtet, eine umfassende Risikobewertung durchzuführen, technische Dokumentationen zu erstellen und eine CE-Kennzeichnung sowie Konformitätserklärung vorzulegen. Die Verordnung tritt am 20. Januar 2027 verbindlich in Kraft. Der CRA hingegen adressiert ausschließlich Produkte mit digitalen Elementen wie Software, IoT-Geräte oder vernetzte Steuerungen. Ziel ist es, diese Produkte gegen Cyberangriffe zu schützen. Hersteller müssen Sicherheitsmaßnahmen wie „Security by Design", ein aktives Schwachstellenmanagement, regelmäßige Sicherheitsupdates und Meldepflichten umsetzen. Auch hier endet die Übergangsfrist Anfang 2027.

Doppelverpflichtung. Besonders relevant ist die Doppelverpflichtung für Hersteller von Maschinen mit digitalen Komponenten. Diese müssen sowohl die Anforderungen der Maschinenverordnung als auch des CRA erfüllen, um ihre Produkte auch nach 2027 rechtskonform in den EU-Markt bringen zu können. Zur Unterstützung bietet TÜV Austria mit seinem Cybersecurity-spezialisten clockworkX GmbH eine praxisnahe CSMS Masterclass an, in der Unternehmen lernen, ein Cybersecurity Management System aufzubauen, das den neuen EU-Vorgaben entspricht. ▮

www.tuvaustria.com

CIS

KI-Ausbildung

© Ela Angerer

„Die Lücke zwischen den schnell wachsenden Anforderungen im KI-Management und dem dafür notwendigen Einsatz und Fachwissen ist derzeit enorm und verunsichert viele Menschen", so **Harald Erkinger,** Geschäftsführer der Certification & Information Security Services GmbH (CIS). Mit der Ausbildung zum KI-Manager sollen die Teilnehmer:innen des KI-Kurses die pragmatische und effektiven Nutzung sowie Integration von KI im eigenen Unternehmen lernen. CIS Certification hat sich schon vor Jahren auf normierte KI-Kompetenzentwicklung in Unternehmen spezialisiert. So wurde das ISO 42001 Zertifikat (Managementsysteme für KI) auch erstmalig von CIS Certification an ein österreichisches Unternehmen verliehen.

www.cis-cert.com

World4you

ÖSTERREICH IST ONLINE

Laut Internet-Kompass von World4you ist das Netz zentrale Informations-, Kommunikations- und Arbeitsplattform. 91 % nutzen es als wichtigste Quelle, 70 % shoppen regelmäßig online.

Österreich ist eine Online-Nation, die im Internet lebt und arbeitet. Das belegt der neue Internet-Kompass des Hosting-Anbieters World4you. Das Internet prägt den Alltag von morgens bis abends und ist auch bei Kaufentscheidungen wichtig. Die Online-Nutzung beginnt für viele schon vor dem ersten Kaffee: Fast die Hälfte der Frauen und 40 % der Männer checken bereits vor dem Frühstück ihre Messenger-Apps. Die Tiroler:innen sind hier mit 53 % federführend im Bundesländervergleich. Auch private E-Mails haben bei 41 % der Befragten, insbesondere bei der Generation 55+, einen festen Platz im Morgenritual, ebenso wie der Tageswetter-Ausblick oder Nachrichten lesen.
Online geht es tagsüber auch weiter. Die Hälfte der Österreicher:innen checkt mindestens zweimal pro Tag seine Mails, jede:r Fünfte unter den Befragten sogar viermal oder häufiger. Das liegt möglicherweise auch an der Vielfalt der Erreichbarkeit. Mit mehr als zwei Dritteln hat die klare Mehrheit der Österreicher:innen zwei oder mehr E-Mail-Adressen.

Digitale Visitenkarte. Geht es darum, sich online über ein Unternehmen zu informieren, bleibt die unternehmenseigene Website die wichtigste Informationsquelle – trotz des rasanten Wachstums von Social Media und Bewertungsportalen: Für 64 % der Befragten ist sie bei der Recherche über ein Unternehmen wichtig – noch vor Bewertungsportalen (60 %) und Social-Media-Profilen (48 %). Besonders die Gruppe der 25- bis 34-Jährigen (69 %) und Männer (67 %) informieren sich vermehrt auf der Unternehmenswebsite. Für die Gruppe der 18- bis 24-Jährigen spielen bei der Recherche für 63 % von ihnen bereits KI-Chatbots eine wichtige Rolle, während sie insgesamt für 39 % der Befragten von Bedeutung sind. „Die Ergebnisse der Umfrage belegen, dass eine professionelle Website für Selbstständige oder Unternehmen heute nach wie vor unverzichtbar ist", sagt Sandra Trummer-Gabler, Geschäftsführerin von World4you. „Eine moderne, sichere und ansprechende Website ist ein verlässlicher Ankerpunkt im Netz und die digitale Visitenkarte eines Unternehmens. Sie schafft Vertrauen und ist das Fundament für den wirtschaftlichen Erfolg eines Unternehmens im Internet."

Basis für Kaufentscheidungen. Vorgelagerte Recherche im Internet ist zudem zum festen Bestandteil des Kaufprozesses geworden: 79 % der Konsument:innen besuchen vor einer Bestellung die Website des Unternehmens. Damit ist die Website ein entscheidender Faktor, der Hand in Hand mit dem Preisvergleich und der Recherche der Zahlungs- und Lieferbedingungen geht. Die Bedeutung von Online-Bewertungen wächst ebenfalls: 77 % der Befragten lassen sich von Bewertungen und Erfahrungen anderer Kund:innen beeinflussen.

Sicherheit im Fokus. Angesichts der intensiven Nutzung des Webs rücken auch die Aspekte Sicherheit und Datenschutz für die meisten Österreicher:innen in den Vordergrund: Datensicherheit ist beim Besuch einer Website nahezu allen ein wichtiges Thema. Knapp zwei Drittel empfinden sie sogar als sehr wichtig. Auch bei der E-Mail-Nutzung sieht trotz der allgemeinen Etabliertheit ein Fünftel von ihnen Bedenken in Sachen Datenschutz und Sicherheit als eine der größten Herausforderungen. Das hohe Aufkommen von Spam-E-Mails zählen 38 % der Befragten dazu. ▮

ww.world4you.com

© RawPixel.com/Freepik

Event

DIGITAL MIT HALTUNG

Der Award „Digitaler Humanismus in der Praxis“ würdigt 2026 erneut Projekte, die zeigen, wie Technologie verantwortungsvoll und im Sinne des Menschen eingesetzt wird. Einreichungen sind ab sofort möglich.

© msg Plaut Austria

Der digitale Wandel braucht Verantwortung und Menschen, die zeigen, wie technologische Innovation im Einklang mit gesellschaftlichen Werten gestaltet werden kann. Um diese Vorbilder sichtbar zu machen und ihr Engagement zu würdigen, wird am 18. März 2026 der Award „Digitaler Humanismus in der Praxis“ zum zweiten Mal verliehen. Damit zeichnen ADV Austrian Digital Value, msg Plaut und Digital Humanism – Verein zur Förderung des digitalen Humanismus Projekte, Organisationen und Persönlichkeiten aus, die zeigen, wie gelebter digitaler Humanismus in Wirtschaft, Verwaltung und Gesellschaft wirkt und wie Technologie zum Wohl des Menschen eingesetzt werden kann.

Starke Partner und hochkarätige Jury. Der Award wird gemeinsam mit Partnern wie ORF, Springer Verlag und den Millstätter Wirtschaftsgesprächen getragen. Die Jury vereint führende Köpfe aus Wirtschaft, Wissenschaft, Verwaltung und Medien – unter anderem Prof. Hannes Werthner (TU Wien), Sabine Herlitschka (Infineon), Gerfried Stocker (Ars Electronica), Patricia Neumann (Siemens), Henrietta Egerth (FFG), Klemens Himpele (CIO Stadt Wien), Michael Heinisch (Vinzenz Gruppe), Vera Treitschke (Springer Verlag), Georg Krause (msg Plaut), Roland Ledinger (BRZ), Erich Prem (Verein Digitaler Humanismus) und Harald Kräuter (ORF).

Einreichung ab sofort möglich. Ab sofort können Unternehmen, Organisationen und Einzelpersonen ihre Beiträge für den Award „Digitaler Humanismus in der Praxis“ 2026 einreichen. Gesucht sind zukunftsweisende Lösungen, Projekte und Initiativen, die gesellschaftlichen Fortschritt mit digitaler Kompetenz verbinden. Eine unabhängige Fachjury bewertet alle Einreichungen nach Innovationsgrad, Wirkung und Nachhaltigkeit.

www.digitalerhumanismus.business

BRZ

ERFOLGREICHE IT-LEHRLINGE

Vier BRZ-Lehrlinge haben ihre Ausbildung erfolgreich abgeschlossen, vier neue starten ins Berufsleben. Das BRZ bietet praxisnahe IT-Ausbildung, Auslandserfahrung und modernste Technologien.

© BRZ/Pineda

Eine Gruppe der erfolgreichen BRZ-Lehrlinge mit Geschäftsführer **Roland Ledinger** (li. außen) und Geschäftsführerin **Christine Sumper-Billinger** (re. außen)

Das BRZ und das Team der Lehrausbilder:innen im BRZ gratulierten im September vier Lehrlingen, die ihre Ausgildung in den Lehrgerufen IT-Sgstemtechnik und Bürokauffrau erfolgreich agschließen konnten und nun ihre Karriere weiterverfolgen. Vor kurzem starteten auch vier neue Lehrlinge ihre Karriere und Ausbildung in den Lehrberufen IT-Systemtechnik, Medienfachkraft Schwerpunkt Grafik und Print sowie im Einkauf. „Eine IT-Lehre bietet eine gute Grundlage für den Eintritt ins Berufsleben. Als Österreichs führender IT-Betrieb im Public Sector bieten wir unseren Lehrlingen nicht nur vom ersten Tag an spannende Herausforderungen sondern auch die Möglichkeit, moderne Technologien und Arbeitsweisen praktisch zu erlernen. Das Angebot, auch Erfahrung im Ausland zu sammeln ist ein weiteres Plus, das unsere Lehrlinge bei entsprechend guten Leistungen gerne in Anspruch nehmen“, so Daniela Mühlberger-Spicker, Bereichsleiterin Human Resources im BRZ.

Internationale Erfahrung. Auch der internationale Austausch wird gefördert. So konnte ein BRZ-Lehrling aus dem Lehrberuf Mediengestaltung kürzlich ein Ausbildungsmonat im spanischen Bilbao verbringen. Ein IT-Systemtechnik-Lehrling aus Norwegen arbeitet derzeit über das Erasmus-Programm für einige Wochen im BRZ. Auf dem TikTok-Kanal des BRZ können Follower:innen Einblicke in das Austauschprogramm erhalten.

www.brz.gv.at

© Freepik

Eset

SICHERHEIT MIT WEITBLICK

Cyberangriffe bedrohen zunehmend kleine und mittlere Unternehmen. Matthias Malcher, Territory Manager Süddeutschland & Österreich bei Eset erklärt, warum IT-Security heute mehr ist als Technik, wie KI Angriffe sowie Schutz verändert und weshalb europäische Lösungen über Wettbewerbsfähigkeit entscheiden.

EHZaustria: ***Viele kleine Unternehmen glauben immer noch, sie seien kein Ziel für Angreifer.***
Matthias Malcher: Das ist ein Irrglaube. Kleine und mittlere Unternehmen sind in Österreich sehr wohl ein attraktives Ziel für Cyberkriminelle. Laut der Studie ‚Cybersecurity in Österreich 2025' von KPMG und weiteren Erhebungen sind bereits rund 32 % der Unternehmen innerhalb der letzten fünf Jahre Opfer von Cyberangriffen geworden – Tendenz steigend. Das Allianz Cyber Risk Barometer 2025 bestätigt, dass Cyberangriffe als das größte Geschäftsrisiko für Unternehmen gelten. Im Bereich Ransomware zeigt das Bundeslagebild Cybercrime 2024 des deutschen Bundeskriminalamts, dass rund 80 % der von Ransomware betroffenen Unternehmen KMU sind. Zudem sehen wir zunehmend Extortion-Angriffe. Dabei werden nicht nur Daten verschlüsselt, sondern gestohlene Daten zur Erpressung angekündigt oder veröffentlicht. Solche Methoden erzeugen enormen Druck auf die Opfer, weshalb auch kleinere Unternehmen Gefahr laufen, zur Zahlung bewegt zu werden.

Der Dschungel an Anbietern und Lösungen ist riesig. Wie findet man da die richtige?
Malcher: Da gibt es natürlich viele Dinge, über die man sich im Vorfeld Gedanken machen muss. Das hängt stark von der jeweiligen Branche ab, vom vorhandenen Budget – nicht jeder kann sich unbegrenzt Security leisten – und auch davon, ob man eine eigene IT-Abteilung hat oder einen IT-Dienstleister beauftragen muss. Eine Risikobewertung ist auf jeden Fall der erste Schritt: Welche Assets sind wirklich kritisch, was muss ich unbedingt absichern, weil es im Ernstfall existenzgefährdend wäre? Wichtig ist außerdem, dass Security mehrschichtig aufgebaut ist. Dabei sollte man unbedingt auf die Interoperabilität der eingesetzten Produkte achten, also ob unterschiedliche Lösungen auch wirklich gut miteinander funktionieren. Wir bei Eset haben zum Beispiel ein Produktbundle speziell für KMU entwickelt, das den Großteil der technischen Anforderungen der NIS-2-Richtlinie abdeckt. Wenn man dann zusätzlich noch Services wie ein Security Operations Center kurz SOC-Service – also eine 24/7-Überwachung – dazu nimmt, muss man sich als Mittelständler eigentlich kaum noch Sorgen um die eigene IT-Security machen. Und ich denke, da sind wir als mittlerweile größter IT-Security-Hersteller in der EU für unsere Kunden eine sehr gute Wahl.

Wie erfolgreich werden Regulierungen wie NIS 2, DORA oder der Cyber Resilience Act künftig sein?
Malcher: Erfolgreich wird die Umsetzung solcher Regularien nur dann sein, wenn sie auch wirklich konsequent umgesetzt und kontrolliert wird. Nur wenn es verbindliche Prüfungen und Nachweise gibt, werden Unternehmen die Vorgaben ernst nehmen und sich entsprechend aufstellen. Die NIS 2 ist dabei im Grunde eine Mindestanforderung an IT-Security. Viele Unternehmen erfüllen heute noch nicht einmal diese Basisvorgaben. Diese Regulierungen helfen oder zwingen Unternehmen, sich intensiver mit Security zu befassen und ihre Strukturen zu verbessern. Ziel ist es ja nicht nur, Angriffe abzuwehren, sondern auch nach einem erfolgreichen Angriff weiter arbeitsfähig zu bleiben. Das heißt, Resilienz aufzubauen, um im Ernstfall nicht tagelang lahm zu liegen oder erst mit einem Incident-Response-Team herausfinden zu müssen, woher der Angriff kam. In diesem Sinne sind diese Regularien ein wichtiger Schritt, um IT-Sicherheit in Europa auf ein neues Niveau zu bringen.

Spüren Sie einen Trend hin zu mehr europäischer Souveränität?
Malcher: Ja, ganz klar. Wir haben derzeit eine sehr hohe Nachfrage nach europäischen Anbietern. Viele Unternehmen wollen sich unabhängiger von US-Herstellern machen – auch, weil die Entwicklung dort schwer einzuschätzen ist, sowohl politisch als auch preislich. Niemand kann vorhersagen, wie sich die Beziehungen zwischen den USA und Europa weiterentwickeln, ob es etwa Strafzölle auf Software geben wird oder ob US-Anbieter wie Microsoft irgendwann den Zugang zu Cloud-Services einschränken könnten. Hinzu kommt die Preispolitik: Große Anbieter erhöhen mehrfach im Jahr die Preise – das ist für viele ein Fass ohne Boden. Deshalb sehen wir eine klare Tendenz, auf EU-Lösungen zu setzen. Diesen Trend bestätigt auch eine Eset-Umfrage dieses Jahr. Von den rund 600 befragten Unternehmen im DACH-Raum haben 75 % angegeben, künftig bewusst auf europäische Hersteller zu setzen.

Oft sind die Ansprüche hoch, aber wenn es ums Geld geht, relativieren sie sich schnell.
Malcher: Niemand kann heute mit Sicherheit sagen, dass nicht irgendwann der Tag kommt, an dem europäische Daten vielleicht doch außerhalb Europas landen oder nicht mehr zugänglich sind. Wir wissen schlicht nicht, wie sich die internationale Lage entwickeln wird oder ob die Daten europäischer Unternehmen wirklich immer und überall zuverlässig zur Verfügung stehen. Genau deshalb wird das Thema „Made in Europe" zunehmend wichtiger. Vielleicht nicht für jedes KMU, aber gerade bei großen Unternehmen sehen wir ein deutlich wachsendes Bewusstsein und eine klare Tendenz, auf europäische Hersteller zu setzen. Für uns bedeutet „Made in Europe", dass unsere Produkte nach europäischen Datenschutzrichtlinien entwickelt werden. Die Entwicklung unserer Lösungen findet vollständig in der EU statt. Als europäischer Hersteller können wir zudem garantieren, dass unsere Produkte keine Backdoors enthalten – also keine versteckten Zugänge für Behörden oder Geheimdienste. Für unsere Kunden in der DACH-Region haben wir im vergangenen Jahr ein eigenes Rechenzentrum in Frankfurt eröffnet. Damit können Unternehmen, die unsere Cloud-Lösungen nutzen, explizit diesen Standort für ihr Hosting wählen und sicherstellen, dass ihre Daten innerhalb Deutschlands gespeichert werden. Denn selbst innerhalb der EU gibt es Unterschiede bei den gesetzlichen Rahmenbedingungen. >>

„Niemand kann heute mit Sicherheit sagen, dass nicht irgendwann der Tag kommt, an dem europäische Daten vielleicht doch außerhalb Europas landen oder nicht mehr zugänglich sind."

Matthias Malcher, Territory Manager Süddeutschland & Österreich bei Eset

© Eset

Aber der Preisunterschied spielt aktuell keine große Rolle. Zumindest im Endpoint-Security-Bereich liegen die Preise von europäischen, amerikanischen, israelischen oder japanischen Herstellern sehr nah beieinander. Der Markt ist extrem hart umkämpft, gerade in Deutschland und Österreich. Das führt letztlich dazu, dass die Kundinnen und Kunden von einem starken Wettbewerb profitieren und sehr gute Konditionen bekommen.

Welche Rolle spielt KI?
Malcher: KI ist definitiv interessant – für Cyberkriminelle genauso wie für die Verteidiger. Schauen Sie sich etwa den Bereich Phishing an. Bei den E-Mails muss man zweimal hinschauen, um zu erkennen, ob sie echt oder ein Angriff sind. Auf der anderen Seite hilft uns KI aber genau dabei, solche Angriffe besser zu erkennen. Gerade bei Incident Response oder der Analyse von Anomalien ist sie eine große Unterstützung. Unsere Kundinnen und Kunden, die etwa Managed Detection and Response einsetzen, profitieren davon besonders, denn so eine Lösung funktioniert nur, wenn sie 24/7 überwacht wird. Cyberkriminelle arbeiten schließlich auch nachts und am Wochenende, viele IT-Abteilungen aber nicht. Über unser SOC in Bratislava bündeln wir international Daten, die per KI und durch ein Team von Analysten ausgewertet werden. So erkennen wir neue Angriffsmuster frühzeitig. Diese Erkenntnisse fließen direkt in unsere Managed Services ein. Das Ergebnis: Ein Frühwarnsystem, das unsere Kundinnen und Kunden aktiv schützt und das zu einem Preis, den sich auch mittelständische Unternehmen leisten können.

Kann durch den Einsatz von KI der Vorsprung, den Cyberkriminelle bislang noch haben, aufgeholt werden?
Malcher: Das ist ein klassisches Katz-und-Maus-Spiel. Ganz schließen kann man diesen Vorsprung wohl nie, aber man rückt mit Hilfe von KI deutlich dichter heran und macht den Abstand spürbar kleiner. Cyberkriminelle nutzen heute meist nicht nur eine einzelne Schwachstelle, sondern eine Kombination mehrerer Sicherheitslücken und Angriffsmethoden, um in ein System einzudringen. Während der Hersteller eines Systems daher gezwungen ist, alle bekannten und unbekannten Sicherheitslücken kontinuierlich zu identifizieren und zu schließen, reicht es für einen Angreifer oftmals sogar aus, nur eine einzige dieser Schwachstellen auszunutzen, um erfolgreich zu sein. Diese Asymmetrie macht es so herausfordernd, Systeme umfassend abzusichern und jederzeit widerstandsfähig gegen Angriffe zu halten. Genau das ist die große Herausforderung: Ein System wirklich umfassend abzusichern, während der Angreifer nur einen kleinen Schwachpunkt finden muss, um erfolgreich zu sein.

Die größte Schwachstelle ist ja oft der Mensch. Man kann technisch alles absichern, und dann klickt trotzdem jemand auf den falschen Link. Wie kann man hier besser sensibilisieren?
Malcher: Man muss das Bewusstsein für Gefahren im Alltag schaffen. Awareness-Trainings sind hier sehr erfolgreich. Es gibt mittlerweile viele Anbieter, die solche Schulungen anbieten und reale Szenarien durchspielen, damit Mitarbeitende lernen, worauf sie achten müssen. Die zweite Komponente ist die technische. Gerade bei Phishing-Mails gibt es heute viele Möglichkeiten, Angriffe frühzeitig zu erkennen. Wenn eine E-Mail mit Anhang eintrifft, wird bei uns zunächst über das cloudbasierte Reputationssystem Eset LiveGrid geprüft, ob die Datei oder ihr Hash bereits bekannt ist. Ist die Datei unbekannt und enthält ausführbaren Code, wird sie automatisch an Eset LiveGuard übermittelt. Dort erfolgt die Ausführung und Verhaltensanalyse der Datei in einer isolierten Cloud-Sandbox, die sowohl physische als auch virtuelle Maschinen nutzt. Die Sandbox-Analyse untersucht das Verhalten der Datei umfassend, um neuartige und bisher unbekannte Bedrohungen sicher zu erkennen und zu blockieren. So ergänzt LiveGuard die erste Prüfung durch LiveGrid um eine tiefgehende Verhaltensanalyse, bevor die Datei am Endpoint freigegeben wird. Wird dabei Schadcode erkannt, entfernen wir die Datei automatisch aus der E-Mail, stellen die Nachricht aber trotzdem zu – mit dem Hinweis, dass der Anhang infiziert war. Das nimmt den Mitarbeitenden viel Verantwortung ab, weil sie so gar nicht erst in die Situation kommen, versehentlich einen Angriff auszulösen.

Zum Abschluss: Wie gestaltet sich die Zusammenarbeit mit dem Channel?
Malcher: Wir verzeichnen in Österreich seit einigen Jahren ein sehr konstantes Wachstum und gewinnen kontinuierlich neue Partner hinzu – vor allem mittelständische und kleinere Systemhäuser. Für unsere Partner bieten wir einen klaren Mehrwert durch kostenlose Schulungen und Zertifizierungen über unsere Trainingsplattform. Darüber hinaus haben wir ein Partnerprogramm, in dem die Partner je nach Partnerstufe selbst steuern können, welche Margen sie mit unseren Produkten erzielen. Ein besonders stark wachsender Bereich ist jener der Managed Service Provider. Immer mehr Systemhäuser stellen ihr Geschäftsmodell um und bieten ihren Kundinnen und Kunden komplette Managed Security Services an. Wir arbeiten in Österreich mit verschiedenen Distributoren zusammen, sowohl mit heimischen als auch mit deutschen, die nach Österreich liefern. Außerdem unterstützen wir die Partner mit unseren eigenen Services, die sie über uns an ihre Endkunden weitergeben können. Dadurch haben heute auch KMU Zugang zu Lösungen, die früher nur Großunternehmen vorbehalten waren. Und das zu leistbaren Konditionen ▮

www.eset.com

Gastkommentar

WARUM KI DIE ZUKUNFT DER CLOUD-TELEFONIE FÜR KMU IST

Cloud-Telefonie trifft Künstliche Intelligenz: Im Gastkommentar von Michael Hengl, Sales Director von Easybell Österreich, zeigt sich, wie KI kleine und mittlere Unternehmen entlastet – für mehr Effizienz, Erreichbarkeit und Wettbewerbsstärke.

© Easybell

„KI ist ein wichtiger Baustein unserer Unternehmensstrategie und damit für die Entwicklung neuer Produkte.“

Michael Hengl,
Sales Director von
Easybell Österreich

Als Sales Director von Easybell in Österreich sehe ich täglich, wie sich die Anforderungen an Unternehmenskommunikation verändern. Gerade kleine und mittlere Unternehmen (KMU) stehen vor einer Herausforderung: Sie müssen professionell erreichbar sein, ohne große Teams oder hohe Budgets. Hier kommt die Kombination aus Cloud-Telefonie und Künstlicher Intelligenz (KI) ins Spiel.
Die Frage, welche Rolle KI bei Easybell spielt, ist schnell beantwortet: Sie ist ein wichtiger Baustein unserer Unternehmensstrategie und damit für die Entwicklung neuer Produkte. Mit unserer offenen Schnittstelle ermöglichen wir es Partnern und Kunden, eigene Voicebots oder andere KI-basierte Lösungen direkt in unsere Cloud-Telefonanlage zu integrieren. Das bedeutet maximale Flexibilität – vom automatisierten Buchungssystem in einer Berghütte bis hin zum digitalen Sekretariat-Service für Handwerker.

Echte Entlastung. Warum ist das so wichtig? Weil KI nicht nur Prozesse automatisiert, sondern echte Entlastung schafft. Ein Voicebot kann Anrufe entgegennehmen, Informationen bereitstellen oder Reservierungen annehmen – rund um die Uhr. Für KMU ist das ein Gamechanger: weniger Personalaufwand, höhere Erreichbarkeit und ein professioneller Auftritt, selbst in Spitzenzeiten.
Mit unserer neuen Funktion innerhalb der Cloud Telefoanlage FQDN (Fully Qualified Domain Name) haben wir die technische Basis geschaffen, um diese Integration noch einfacher und sicherer zu machen. Unternehmen können ihre individuellen KI-Dienste nahtlos anbinden, ohne komplexe Konfigurationen. Das ist unser Ansatz: Offenheit, Partnerschaft und Zukunftsfähigkeit.
Die nächsten Jahre werden zeigen, wie stark KI die Kommunikation prägt. Für uns ist klar: Wer heute auf intelligente Cloud-Telefonie setzt, hat morgen einen entscheidenden Wettbewerbsvorteil. ▮

www.easybell.de

Exclusive Networks

ERWEITERTE PARTNERSCHAFT

Exclusive Networks und Drata erweitern ihre strategische Partnerschaft auf die DACH-Region, Großbritannien, Irland und die nordischen Länder.

Exclusive Networks und Drata arbeiten bereits seit längerem erfolgreich zusammen. Bisher war die Kooperation auf die Benelux-Länder fokussiert. Durch die umfangreichere Partnerschaft werden die Lösungen von Drata nun auch für IT-Händler und Managed Service Provider (MSPs) in der DACH-Region sowie in Großbritannien, Irland und den nordischen Ländern verfügbar sein. Durch die Integration in das Partner-Ökosystem von Exclusive Networks wird die KI-gestützte Plattform von Drata zur Vereinfachung und Skalierung von Compliance-Prozessen einer weiteren umfangreichen Unternehmensgruppe zugänglich.

Compliance-Co-Pilot. Die Lösung von Drata überwacht die Sicherheitsmechanismen von Unternehmen und sammelt automatisiert entsprechende Nachweise wie Passwort-Policies und Zugriffskontrollen für externe Prüfer. Gleichzeitig werden Compliance-Workflows vollständig optimiert, das Monitoring findet kontinuierlich statt und bereitet automatisiert auf anstehende Audits vor. Die Plattform mit dieser automatisierten Beweissicherung und den Echtzeit-Risikomanagementfunktionen eignet sich für Unternehmen jeder Größe, die damit ihre Compliance langfristig aufrechterhalten und gleichzeitig den manuellen Aufwand und die Betriebskosten reduzieren können. „Drata positioniert sich als Compliance-Co-Pilot, der den bürokratischen Aufwand in Unternehmen reduziert und viele Risiken reduziert“, erklärt Marcus Adä, General Manager Germany und Regional Manager DACH und sagt weiter: „Damit ist Drata eine weitere wichtige Erweiterung unseres umfassenden Cybersecurity-Portfolios – und ein strategischer Baustein, um unsere Partner in der DACH-Region noch besser dabei zu unterstützen, die steigenden Anforderungen an Compliance und Sicherheit zuverlässig und effizient zu erfüllen.“

www.exclusive-networks.com

© Exclusive Networks

„Drata positioniert sich als Compliance-Co-Pilot, der den bürokratischen Aufwand in Unternehmen reduziert und viele Risiken reduziert.“

Marcus Adä,
General Manager Germany und Regional Manager DACH

Systeam

Philips Monitore im Sortiment

Ab sofort vertreibt Systeam das gesamte Portfolio an B2B- und B2C-Modellen von Philips Monitore und Gaming Displays der Marke Philips Evnia in Deutschland. Das wurde durch die neue Distributionspartnerschaft mit MMD, Markenlizenzpartner für Philips Monitore, möglich. Die Zusammenarbeitet startet pünktlich zum 40-jährigen Firmenjubiläum von Systeam und fällt gleichzeitig mit dem Launch des neuen SMB-Partnerprogramms von MMD speziell für kleine und mittelständische Unternehmen zusammen. Mit der Aufnahme der leistungsstarken Displays im modernen, eleganten Design von Philips Monitore will der oberfränkische Distributor sein breites Angebot im Bereich IT und AV weiter ausbauen. „Systeam ist ein starker Partner mit exzellentem Marktzugang, insbesondere zum Mittelstand. Dank unseres neuen SMB-Partnerprogramms und der geballten Vertriebskompetenz von Systeam werden wir unsere Sichtbarkeit und Marktdurchdringung in Deutschland signifikant erhöhen. Wir freuen uns auf eine langfristige, partnerschaftliche Zusammenarbeit“, erklärt Lutz Hardge, Regional Sales Director DACH bei MMD. Auch bei Systeam ist man überzeugt vom Mehrwert der Kooperation. „Philips Monitore stehen für Qualität, Innovation und ein erstklassiges PreisLeistungs-Verhältnis – genau das, was unsere Fachhandelspartner erwarten“, sagt Dominik Dütsch, Produktmanager bei Systeam. „Ob für den effizienten Workflow im modernen Arbeitsumfeld oder für immersives Gaming in der Pause – mit dieser Sortimentserweiterung können wir noch gezielter auf die Bedürfnisse unserer Kunden eingehen.“

www.systeam-austria.at

© Systeam

V.l.n.r.: **Dominik Dütsch, Miriam Hirschi, Lutz Hardge** (MMD), **Volker Mitlacher, Lars Michelsen** (MMD), **Stefanie Hoydem** und **Matthias Mitlache**r (wenn nichts anderes angegeben, Systeam)

Interview

SICHER UND ERFOLGREICH IN DIE AWS EUROPA CLOUD

AWS bringt mit der European Sovereign Cloud eine sichere, EU-konforme Cloud. ByteSource begleitet Unternehmen mit Expertise in Compliance und DevOps. Alexander Penev, CEO und Gründer von ByteSource erklärt die Details.

AWS als einer der weltweit führenden Hyperscaler plant Ende 2025 die European Souvereignty Cloud (ESC) einzuführen. Was ist das genau und was bedeutet das für Europa?
Alexander Penev: Die AWS European Sovereign Cloud ist eine speziell entwickelte Infrastruktur, die den strengen Anforderungen der EU an Datenhoheit und Regulierung gerecht wird. Sie richtet sich an öffentliche Einrichtungen sowie an Unternehmen aus stark regulierten Branchen wie Finanzwesen, Gesundheitswesen und Telekommunikation. Die Cloud bietet dieselben Services, APIs, Architekturen und Sicherheitsstandards wie die globale AWS Cloud – jedoch mit vollständiger Unabhängigkeit von bestehenden AWS-Regionen. Zur Gewährleistung einer autonomen Governance hat AWS eine dedizierte europäische Organisation gegründet, bestehend aus einer Muttergesellschaft und drei Tochtergesellschaften mit Sitz in Deutschland. Diese Struktur wird von EU-Bürger:innen mit Wohnsitz in der EU geleitet und ist für Compliance, Betrieb und Sicherheit gemäß europäischen Rechtsstandards verantwortlich.

Was bedeutet das für ESC-Kunden und was ist der Beitrag von ByteSource?
Penev: Mit der AWS European Sovereign Cloud setzt AWS einen neuen Maßstab für sichere, autonome und skalierbare Cloud-Infrastrukturen in der EU. Sie ermöglicht es Kunden, mit Vertrauen zu innovieren – im Wissen, dass ihre Daten und Betriebsabläufe vollständig unter europäischer Rechtshoheit stehen. Die ByteSource Technology Consulting GmbH ist Österreichs AWS Advanced Tier Services Partner und nimmt eine führende Rolle im Cloud-Ökosystem ein. Als erster und einziger Partner mit AWS DevOps Competency und erster Partner mit AWS Generative AI Competency verfügen wir über ein einzigartiges Kompetenzprofil und begleiten Unternehmen umfassend auf ihrer Cloud Journey – von der Strategie über die Migration bis hin zu Betrieb und Modernisierung. Unsere strategische Differenzierung basiert auf langjähriger Erfahrung in hochregulierten Branchen wie Banken, Versicherungen und dem öffentlichen Sektor sowie auf tiefem Know-how in Data Residency, Compliance und europäischen Datenschutzanforderungen. Wir entwickeln DSGVO-, NIS2- und KRITIS konforme Architekturen, sind vertrauenswürdiger Partner öffentlicher Institutionen, betreiben Enterprise-Scale Operations für internationale Kunden wie die BMW Group und setzen auf einen konsequenten DevOps- und Security-First-Ansatz mit umfassender wModernisierungskompetenz. Die AWS European Sovereign Cloud schafft optimale Voraussetzungen für vielfältige Anforderungen – und mit unserer langjährigen Erfahrung sind wir der ideale Partner für die erfolgreiche Umsetzung.

Wie unterstützt ByteSource die Kunden bei der Journey in die AWS Cloud?
Penev: Wir begleiten unsere Kunden auf ihrem Weg in die AWS European Sovereign Cloud und durch die Souveränitätskontrollen. Unser erfahrenes Team unterstützt End-to-End – von sicherer Architektur und Governance über compliance-fähiges DevOps bis hin zu resilienten Migrationsstrategien und kosteneffizientem Betrieb. Als größter Atlassian Partner Österreichs verbinden wir zusätzlich Cloud-Native-Architekturen mit modernen Kollaborations- und DevOps-Plattformen. ByteSource Technology Consulting GmbH ist einer der führende AWS-Partner in Österreich und einer der profiliertesten Cloud- und DevOps-Spezialisten im DACH-Raum. Mit Standorten in Wien und München begleiten wir Unternehmen aus allen Branchen – von Start-ups bis zu multinationalen Konzernen – auf ihrer Cloud Journey.

www.bytesource.net

Alexander Penev,
CEO und Gründer von ByteSource

© ThomasUnterberger

T-Systems Austria

SOUVERÄN IN DER CLOUD

Europa holt technologisch auf – davon ist DI Eduard Kowarsch, Head of Cloud Services bei T-Systems Austria, überzeugt. Im Interview spricht er über Abhängigkeiten von Asien und den USA, über Chancen europäischer Cloud-Anbieter und wie T-Systems zur digitalen Souveränität beitragen will.

© Freepik

EHZaustria: ***Wo sehen Sie aktuell die größten Herausforderungen für Unternehmen, die in die Cloud wollen?***
Eduard Kowarsch: Die sind vielfältig. Ein wesentlicher Punkt ist die Frage, ob die Applikationen, die ein Unternehmen für sein Geschäft braucht, überhaupt cloudfähig sind. Das wird häufig unterschätzt, vor allem, wenn man sich bisher wenig mit dem Thema Cloud beschäftigt hat. Man muss sich zunächst genau ansehen: Welche Anwendungen nutze ich eigentlich? Gibt es dafür eine Standardvariante, die in der Cloud läuft? Oder handelt es sich um Eigenentwicklungen, die erst angepasst werden müssen, um in der Cloud betrieben werden zu können? „Lift and Shift" – also das Verschieben bestehender Systeme eins zu eins vom eigenen Rechenzentrum in die Cloud funktioniert zwar grundsätzlich, ist aber meist ineffizient und teuer. Ein weiterer Punkt ist der geografische Bedarf: Wenn ich meine Anwendungen nur an einem Standort benötige und keine europa- oder weltweiten Zugriffe brauche, muss man sich gut überlegen, ob sich der Schritt in die Cloud lohnt. Und schließlich spielt auch die Latenz, also die Antwortzeit der Systeme, eine wichtige Rolle. In der Fertigungsindustrie etwa kann eine Cloud-Lösung problematisch sein, wenn die Verbindung zu langsam oder instabil ist – etwa bei einer Produktionssteuerung, die in Echtzeit reagieren muss. Fällt die Netzwerkverbindung aus, steht im schlimmsten Fall die gesamte Anlage. Diese Kriterien sollte man daher immer sorgfältig prüfen, bevor man sich für den Schritt in die Cloud entscheidet.

Gibt es eine Empfehlung, wann Private Cloud, wann Public Cloud oder eine hybride Lösung sinnvoll ist?
Kowarsch: Grundsätzlich empfehlen wir immer, mit einem Beratungsprojekt zu starten. Dabei analysieren wir gemeinsam mit dem Kunden die bestehende IT-Landschaft und entwickeln, falls noch nicht vorhanden, eine Cloud-Strategie. Es geht darum zu klären, was überhaupt in die Cloud gebracht werden soll, was technisch möglich ist, welche Applikationen im Einsatz sind, wie geschäftskritisch sie sind und welche Lastverhältnisse bestehen. Auf Basis dieser Analyse lässt sich dann entscheiden, wo welche Systeme am besten betrieben werden. Ein Thema, das zunehmend wichtiger wird, ist die Souveränität. Gemeinsam mit der Deutschen Telekom haben wir definiert, was wir darunter verstehen und drei Kategorien festgelegt. Die erste ist Datensouveränität, also die Hoheit über die eigenen Daten. Ziel ist, sicherzustellen, dass niemand unbefugt auf Daten zugreifen oder sie verwenden kann. Das lässt sich etwa durch Verschlüsselung erreichen – so können Daten auch in einer Public Cloud gespeichert werden, solange der Schlüssel beim Kunden bleibt. Die zweite Kategorie ist die Betriebssouveränität. Dabei geht es um die Frage, wer die Cloud-Infrastruktur tatsächlich betreibt. Die dritte Kategorie ist die technologische Souveränität und die ist am schwierigsten sicherzustellen. Bei Software kann man sich durch Open-Source-Lösungen unabhängiger machen, aber bei Hardware ist es derzeit praktisch unmöglich, europäische Server zu beziehen. Europa arbeitet daran, eine eigene Produktionsbasis wieder aufzubauen, aber das wird sicher noch viele Jahre dauern. Bis dahin setzen wir auf Server amerikanischer oder asiatischer Hersteller – achten aber darauf, die größtmögliche Unabhängigkeit zu gewährleisten.

Wird das Souveränitäts-Thema aktiv nachgefragt oder ist es eher ein Angebot von Ihrer Seite?
Kowarsch: Das Interesse hat in den letzten Jahren deutlich zugenommen – allerdings unterscheiden sich die Branchen hier stark. Im Public Sector hat das Thema eine besonders große Bedeutung, weil dort ein ganz anderes Bewusstsein für Datensouveränität herrscht. Wir haben mehrfach erlebt, dass öffentliche Einrichtungen, die kurz davor waren, Workloads in eine Public Cloud zu verlagern, den Schritt noch einmal gestoppt und Alternativen geprüft haben. Sehr ausgeprägt ist das Thema auch im Gesundheitssektor, wo es um hochsensible Daten geht. Dort ist die Nutzung einer Public Cloud oft schwer darstellbar. Ähnlich ist es bei Banken und Versicherungen. Auch sie müssen regulatorisch sicherstellen, dass es Alternativen zu amerikanischen Cloud-Anbietern gibt. Selbst wenn sie Azure, AWS oder Google einsetzen, brauchen sie also eine zweite, souveräne Lösung als Plan B. In der privaten Wirtschaft, etwa im Manufacturing-Bereich, ist Souveränität ebenfalls ein Thema, steht aber meist nicht an erster Stelle. Hier geht es oft stärker um das Preis-Leistungs-Verhältnis.

Was wird europäische Cloud-Anbieter künftig von den großen internationalen unterscheiden?
Kowarsch: Eine europäische Cloud zeichnet sich dadurch aus, dass sie alle europäischen Zertifizierungen vollständig erfüllt – und zwar wirklich bis zum Maximum. Dazu gehören selbstverständlich die DSGVO, aber auch zahlreiche Sicherheitszertifizierungen sowie regulatorische Vorgaben, etwa von der Finanzaufsicht oder aus dem Gesundheitsbereich. All das ist bei uns von Beginn an built-in – also integraler Bestandteil unserer Cloud-Angebote. Ein weiterer großer Unterschied zu den amerikanischen Hyperscalern ist der Umgang mit Datenhoheit. Dort ist es oft leicht, Daten in die Cloud zu bringen, aber schwer, sie wieder herauszubekommen – ein klassisches Lock-in-Szenario. Bei uns ist das anders: Wir setzen konsequent auf Souveränität und Unabhängigkeit. Unsere Lösungen basieren auf Open-Source-Software, die frei verfügbar ist. Unser Ziel ist nicht, Kundinnen und Kunden an uns zu binden, sondern sie mit gutem Service und Qualität zu überzeugen damit sie freiwillig bleiben.

„Wir setzen konsequent auf Souveränität und Unabhängigkeit."
DI Eduard Kowarsch,
Head of Cloud Services bei T-Systems Austria

© T-Systems Austria

Wie konnte es überhaupt so weit kommen, dass andere Regionen – insbesondere die USA und Asien – eine derartige Vormachtstellung haben, während Europa erst in den letzten Jahren versucht, aufzuholen?
Kowarsch: Das hat mehrere Gründe. Zum einen liegen die Fertigungskosten in Asien deutlich unter denen in Europa. Aber auch die USA sind in der Hardwareproduktion stark von Asien abhängig. Es handelt sich also in erster Linie um ein kommerzielles Thema: Aus Kostengründen wurde die Produktion in vielen Branchen nach Asien verlagert. Früher wurden auch in Europa Chips und Computer hergestellt, aber das ist heute weitgehend verschwunden. Zum anderen spielt auch die Art und Weise eine Rolle, wie amerikanische Konzerne agiert haben. Sie haben Marktnischen sehr geschickt erkannt und genutzt, um rasch weltweit eine dominante Marktposition zu erreichen.

Wie wichtig ist die Cloud im Portfolio von T-Systems?
Kowarsch: Viele Unternehmen gehen ganz klar in Richtung Cloud und das lässt sich auch nicht aufhalten. Deshalb hat sie für uns eine hohe Bedeutung. Wir fassen unsere Cloud-Lösungen unter T-Cloud zusammen und unterscheiden dabei drei Kategorien. Erstens die T-Cloud Public: das ist unsere Open Telekom Cloud, basierend auf OpenStack. Die zweite Kategorie ist T-Cloud Privat. Sie ist eine Private Cloud in unseren Rechenzentren und etwa für SAP- oder andere Workloads gedacht. Die T-Cloud Sovereign als dritte Kategorie ist für besonders kritische Anwendungen gedacht, zum Beispiel im Gesundheitswesen oder bei Versicherungen, wo sehr sensible Daten verarbeitet werden. Hier investieren wir stark und stellen auch viel Rechenleistung für AI zur Verfügung und bauen diese Strategie mit den drei Souveränitätsstufen konsequent weiter aus.

Sie sprechen AI an. Damit steigt automatisch der Bedarf an Rechenleistung. Wie wird sich das auf Rechenzentren auswirken?
Kowarsch: Das ist ein ganz wichtiger Punkt für die Zukunft. AI ist in aller Munde, und wir stehen dabei noch ganz am Anfang. Da wird sich noch sehr viel tun. Viele nutzen AI heute schon für einzelne Themen und das wird weiter zunehmen – damit steigt natürlich auch der Bedarf an Rechenleistung. Für AI-Workloads werden spezielle Chips benötigt, sogenannte GPUs, während für klassische Workloads weiterhin CPUs eingesetzt werden. Diese haben wir bereits, aber die Nachfrage wird weiter steigen. Aktuell geht es vor allem darum, GPUs in die Rechenzentren zu bringen und bereitzustellen. Daran arbeiten wir intensiv, haben bereits entsprechende Kapazitäten aufgebaut und errichten in Deutschland eine AI Industry Factory, um gezielt AI-Workloads bedienen zu können. Ab dem nächsten Jahr werden wir dort rund 10.000 NVIDIA-GPUs für den Markt zur Verfügung haben. Zusätzlich haben wir uns am europäischen Programm der AI Giga Factories beteiligt. Dort geht es darum, europaweit rund 100.000 NVIDIA-GPUs bereitzustellen. Dieses Projekt wird von der EU gesteuert und soll sicherstellen, dass Europa über ausreichend Rechenzentren mit spezialisierter AI-Leistung verfügt.

www.t-systems.at

© pikisuperstar/Freepik

© TD Synnex

TD Synnex

ERWEITERTES MANAGED PRINT PORTFOLIO

TD Synnex und Vasion bündeln ihre Kräfte. Durch eine neue Distributionsvereinbarung soll die Präsenz des Anbieters cloudbasierter Druck- und Dokumentenlösungen in der DACH-Region wachsen.

TD Synnex schließt mit Vasion (vormals PrinterLogic), einem Anbieter cloudbasierter Lösungen für Druckmanagement und die Automatisierung von Dokumentenprozessen, eine Distributionsvereinbarung. Vasions Präsenz soll dadurch in Deutschland, Österreich und der Schweiz weiter ausgebaut werden. Ziel der strategischen Partnerschaft ist der gemeinsame Aufbau eines leistungsstarken Channel-Netzwerks aus Systemhäusern, Value Added Resellern (VARs) und Managed Service Providern (MSPs). Daniel Zenz, Sr. Director Endpoint Solutions der TD Synnex Austria, kommentiert die Vertragsunterzeichnung: „Wir freuen uns sehr über die Erweiterung unserer bereits erfolgreichen Partnerschaft mit Vasion nun auch auf die DACH-Region. In den USA arbeiten wir schon seit mehreren Jahren eng zusammen und haben nun diese Beziehung auch auf Europa erweitert – denn wir sind überzeugt von der Innovationskraft und Leistungsfähigkeit der Lösungen. Mit den Vasion Lösungen wird Druckmanagement für unsere Vertriebspartner und deren Kunden nicht nur einfacher – sondern auch smarter, skalierbarer und zukunftssicher für die Anforderungen moderner Arbeitswelten.“ Thomas Zirpel, Channel Account Manager für die DACH-Region bei Vasion, erklärt: „Mit TD Synnex haben wir einen starken, etablierten Distributionspartner an unserer Seite, der über exzellente Marktkenntnis, ein umfangreiches Partnernetzwerk und große Erfahrung im Cloud-Bereich verfügt. Diese Zusammenarbeit ist ein entscheidender Schritt, um unsere Sichtbarkeit im Markt zu erhöhen und den Aufbau langfristiger, strategischer Partnerschaften mit VARs, Systemintegratoren und MSPs zu beschleunigen.“

Zentrale Verwaltung. Vasion bietet auf seiner KI-unterstützten SaaS-Plattform derzeit ein cloudnatives Print- und Outputmanagement sowie eine Lösung zur Automatisierung von Dokumentenprozessen an. Mit Vasion können Unternehmen lokale Druckserver abschaffen und Direct-IP-Drucker zentral verwalten – unabhängig von Standort, Hersteller, Betriebssystem und ID-Provider. IT-Abteilungen profitieren von automatisierter Treiberbereitstellung, rollenbasierter Zugriffskontrolle und einer intuitiven Self-Service-Oberfläche, die Supportanfragen deutlich reduziert. Dadurch lassen sich Kosten senken, Ressourcen effizienter nutzen und die Skalierbarkeit erhöhen. Die Plattform ermöglicht zudem zentrale Kontrolle, KI-gestützte Workflows und eine nahtlose Integration in Systeme wie SAP, Oracle, Epic und viele andere.

Gerade in hybriden Arbeitsumgebungen schafft Vasion eine flexible und sichere Infrastruktur, die sich nahtlos in bestehende Systeme integrieren lässt. Die Lösung unterstützt Zero Trust-Strategien, reduziert Sicherheitsrisiken und sorgt für eine spürbare Entlastung der IT-Ressourcen. Unternehmen berichten von bis zu 90 % weniger Helpdesk-Tickets und einer deutlich gesteigerten Produktivität. ▮

https://at.tdsynnex.com/

„Mit den Vasion Lösungen wird Druckmanagement für unsere Vertriebspartner und deren Kunden nicht nur einfacher – sondern auch smarter, skalierbarer und zukunftssicher für die Anforderungen moderner Arbeitswelten.“

Daniel Zenz,
Sr. Director Endpoint Solutions der TD Synnex Austria

Zoom

ÜBERARBEITETES PARTNERPROGRAMM

Zoom hat sein globales Partnerprogramm grundlegend überarbeitet. Das neue „Zoom Up“-Modell setzt auf Flexibilität, Transparenz und individuelle Leistung – mit klaren Vorteilen für Partner und Kunden sowie einem modernen Punktesystem statt starrer Strukturen.

„Unser bisheriges Partnerprogramm hat uns in der Anfangsphase gute Dienste geleistet, war jedoch nicht darauf ausgelegt, mit der Vielfalt und dem Wachstum unseres globalen Partner-Ökosystems Schritt zu halten. Es schränkte unsere Möglichkeiten ein, den vollen Wert unserer Partner anzuerkennen“, so Nick Tidd, Head of Global Channel GTM bei Zoom. „Wir haben einen klaren Bedarf für ein flexibleres, transparenteres und leistungsorientierteres Modell gesehen, das es unseren Partnern ermöglicht, mit uns zu wachsen und es Kunden gleichzeitig erleichtert, zum richtigen Zeitpunkt das richtige Know-how zu finden.“

Viele neue Vorteile. Zu den wichtigsten Neuerungen des Zoom-Up-Partnerprogramms zählen etwa getrennte Tracks für Reseller und Agenturpartner. Das bedeutet: Partner werden künftig auf separaten, auf ihr Geschäftsmodell zugeschnittenen Tracks bewertet, sodass Leistung und Vergütung entsprechend ihres Geschäftsmodells angepasst werden können. Anstelle eines starren Checklisten-Modells setzt Zoom künftig auf ein dynamisches Punktesystem. Partner können Punkte für Aktivitäten sammeln, die am besten zu ihren individuellen Geschäftszielen passen. Außerdem wird das Zoom Services Certification Program in Zoom Up integriert und mit bestehenden Vertriebskompetenzen kombiniert. Partner werden für ihre spezifischen Fachgebiete anerkannt. Zoom definiert und kommuniziert künftig den Mehrwert der einzelnen Programmniveaus klar gegenüber Kunden, damit diese rasch den passenden Partner finden. Ergänzt wird alles um ein neues Partner-Dashboard, das Komplexität reduzieren und es Partnern ermöglichen soll, ihre Ziele und Erfolge auf einen Blick zu sehen. ▮

https://partner.zoom.com/

© Freepik

© Red Hat

Hans Roth,
Senior Vice President & General Manager EMEA, Red Hat

Red Hat

Für mehr Unabhängigkeit

Um dem Ruf nach digitaler Souveränität in Europa gerecht zu werden, kündigt Red Hat seinen „Red Hat Confirmed Sovereign Support“ an. Das neue Support-Angebot wurde speziell entwickelt, um technischen Support innerhalb der EU für Software-Subskriptionen von Red Hat bereitzustellen. Damit soll ein neues Maß an, überprüfbarer lokaler Kontrolle über kritische IT-Vorgänge ermöglicht werden. Das Angebot baut auf der mehr als zehnjährigen Erfahrung des Open-Source-Spezialisten bei der Bereitstellung von Support-Modellen für bestimmte Regionen und Branchen auf, insbesondere für Unternehmen, die in stark regulierten Märkten tätig sind oder strenge Compliance-Anforderungen erfüllen müssen. „Red Hat investiert klar und deutlich in die digitale Souveränität Europas. Europäische Unternehmen benötigen Kontrolle über ihre Infrastruktur, und diese Kontrolle muss bei den Menschen beginnen, die sie unterstützen. Mit Red Hat Confirmed Sovereign Support gehen wir direkt auf diese Forderung ein, indem wir ein von EU-Bürgern geleitetes Support-Team und einen entsprechenden Workflow für unsere Open-Source-Lösungen für Unternehmen bereitstellen“, erklärt Hans Roth, Senior Vice President & General Manager EMEA, Red Hat. „Dieses Angebot unterstreicht das Engagement von Red Hat, EU-Unternehmen in die Lage zu versetzen, ihre digitale Zukunft selbst zu gestalten und auf unserem offenen Hybrid-Cloud-Fundament aufzubauen, um mehr digitale Autonomie und Resilienz zu erreichen.“ Der Support wird ab Anfang 2026 verfügbar sein.

www.redhat.com

FORTINET: SICHERHEIT OHNE KOMPROMISSE – DIE ARCHITEKTUR FÜR EINE VERNETZTE ZUKUNFT

Fortinet ist einer der weltweit führenden Anbieter von Cybersecurity-Technologien und hat sich seit seiner Gründung im Jahr 2000 durch Ken und Michael Xie als Pionier für integrierte Netzwerksicherheit etabliert.

Fortinet bietet ein umfassendes Portfolio an Sicherheitslösungen, die sich durch hohe Performance, Skalierbarkeit und Integration auszeichnen. Die Vision des Unternehmens ist klar: eine vernetzte Welt, in der Sicherheit nicht als Hindernis, sondern als Enabler für Innovation und Wachstum verstanden wird. Die Lösungen von Fortinet decken alle relevanten Bereiche der modernen IT-Sicherheit ab – von Netzwerkschutz über Cloud-Security bis hin zu Zero Trust und Operational Technology.

Im Zentrum steht die Fortinet Security Fabric, eine offene, adaptive Plattform, die verschiedene Sicherheitskomponenten miteinander verbindet und eine ganzheitliche Sicht auf Bedrohungen und Schutzmaßnahmen ermöglicht. Die Fabric integriert Firewalls, Switches, Access Points, Endgeräte, Cloud-Ressourcen und Anwendungen in eine zentrale Architektur, die über FortiManager und FortiAnalyzer orchestriert wird. Für Techniker bedeutet das: weniger Silos, mehr Transparenz und eine deutlich schnellere Reaktion auf Sicherheitsvorfälle. Für IT-Reseller entsteht ein Portfolio, das sich modular vermarkten lässt und hohe Kundenbindung erzeugt. Endkunden profitieren von einer Sicherheitslösung, die sich an ihre Umgebung anpasst und kontinuierlich lernt.

Ein zentrales Produkt ist die FortiGate Next Generation Firewall, die physisch und virtuell verfügbar ist und Funktionen wie Deep Packet Inspection, SSL-Entschlüsselung, Intrusion Prevention, VPN und Application Control vereint. Die Appliances sind für kleine Büros ebenso geeignet wie für große Rechenzentren und bieten Hochverfügbarkeit, Clusterbetrieb und granulare Richtliniensteuerung. Besonders hervorzuheben ist die Integration mit FortiGuard Security Services, die Bedrohungsdaten in Echtzeit liefern und Schutz vor bekannten und unbekannten Angriffen bieten. Für Techniker bedeutet das: eine zentrale Steuerung, automatisierte Reaktion und eine Plattform, die Bedrohungen erkennt, bevor sie aktiv werden. Damit entsteht ein Sicherheitsnetz, das nicht nur schützt, sondern auch informiert.

Auch im Bereich Cloud-Sicherheit bietet Fortinet umfassende Lösungen. Mit FortiGate VM, FortiCNP und FortiWeb Cloud lassen sich Public-Cloud-Umgebungen wie AWS, Azure und Google Cloud ebenso absichern wie private Cloud-Infrastrukturen. Die Plattform bietet Funktionen wie Cloud-native Firewalling, API-Schutz, Compliance-Reporting und Zugriffskontrolle. Für Techniker bedeutet es: weniger manuelle Eingriffe, bessere Kontrolle und eine Plattform, die mit der Cloud wächst. Fortinet bietet Kunden die Sicherheit, dass ihre Daten auch in fremden Infrastrukturen geschützt bleiben.

Ein weiteres Highlight ist Fortinet Unified SASE, eine cloudbasierte Architektur, die SD-WAN, Secure Web Gateway, Cloud Access Security Broker, Zero Trust Network Access und Firewall-as-a-Service miteinander kombiniert. Die Lösung ist ideal für Unternehmen mit verteilten Standorten und hybriden Arbeitsmodellen und bietet sichere, performante Verbindungen – unabhängig von Ort und Gerät. Für Techniker bedeutet das: eine zentrale Steuerung aller Netzwerkzugriffe, automatisierte Richtlinien und eine Plattform, die sich flexibel anpasst. Das Produkt lässt sich auch als Managed Service betreiben. Kunden profitieren von einer Lösung, die Sicherheit und Konnektivität vereint.

Fortinet bietet darüber hinaus Lösungen für Endpoint-Schutz, E-Mail-Sicherheit und Web Application Firewalls. Mit FortiClient, FortiEDR, FortiMail und FortiMail Workspace Security lassen sich Endgeräte, Kommunikation und Anwendungen effektiv absichern. Die Plattformen sind mandantenfähig, skalierbar und bieten ein hohes Maß an Automatisierung. Für Techniker bedeutet das: weniger Aufwand, bessere Erkennung und eine Plattform, die sich in bestehende Workflows integriert. Kunden profitieren von sicherer Kommunikation und einem Schutz, der mit der Bedrohungslage wächst.

Ein besonderes Augenmerk legt Fortinet auf Operational Technology (OT) und industrielle Netzwerke. Mit FortiNAC, FortiSwitch und FortiSIEM lassen sich ICS- und SCADA-Umgebungen segmentieren, überwachen und absichern. Die Plattform bietet Deep Packet Inspection für industrielle Protokolle, zentrale Sichtbarkeit und automatisierte Reaktion. Für Techniker bedeutet das: eine zentrale Steuerung aller OT-Komponenten, weniger Angriffsfläche und eine Plattform, die auf zukünftige Herausforderungen vorbereitet. Dadurch entsteht ein Sicherheitsrahmen, der nicht nur schützt, sondern auch die Geschäftskontinuität sicherstellt.

Fortinet setzt stark auf KI und Automatisierung. Die FortiAI-Engine analysiert kontinuierlich das Verhalten von Nutzern, Geräten und Anwendungen und erkennt Anomalien in Echtzeit. Die Plattform lernt mit jeder neuen Bedrohung und passt Schutzmechanismen automatisch an. Die Lösungen sind DSGVO-konform, unterstützen Zero Trust und bieten eine durchgängige Sicht auf alle Ebenen der Infrastruktur. Das bedeutet weniger manuelle Eingriffe, schnellere Reaktion und ein Sicherheitsniveau, das mit den Angreifern Schritt hält.

Die Plattform ist vollständig cloudfähig, unterstützt hybride Bereitstellungen und bietet rollenbasierte Dashboards, automatisierte Reports und Echtzeit-Monitoring. Die Benutzeroberfläche ist intuitiv, die Konfiguration flexibel und die Skalierbarkeit hoch. Fortinet bietet darüber hinaus Schulungen, Support und ein aktives Partnernetzwerk, das Implementierung und Betrieb unterstützt. Das bringt viele Mehrwerte, wie schnelle Time-to-Value, hohe Kundenzufriedenheit und langfristige Bindung. Für Techniker entsteht eine Plattform, die nicht nur funktioniert, sondern auch begeistert. Kunden erhalten eine Lösung, die ihre digitale Resilienz stärkt und ihre strategischen Ziele unterstützt. ▮

Executive Summary: Die wichtigsten Merkmale von Fortinet

- Fortinet Security Fabric als integrierte Sicherheitsarchitektur
- FortiGate NGFW mit Deep Packet Inspection und FortiGuard Services
- Cloud-Security für AWS, Azure, GCP und private Clouds
- Unified SASE mit SD-WAN, ZTNA und CASB
- KI-gestützte Bedrohungserkennung mit FortiAI
- OT-Security für industrielle Netzwerke und kritische Infrastrukturen
- Endpoint-, E-Mail- und Web-Security mit FortiClient, FortiMail und FortiWeb
- FortiMail Workspace Security für Browser-Security und Advanced Threat Protection
- Mandantenfähigkeit, API-Integration und rollenbasierte Dashboards
- Cloud-native Architektur mit DSGVO-Konformität und Zero Trust
- Strategischer Fokus auf Resilienz, Skalierbarkeit und digitale Transformation

Distribution in Österreich:

Die Distribution von Fortinet für den Channel erfolgt durch die Arrow ECS GmbH.

Arrow ECS GmbH
office.ecs.at@arrow.com
Tel. +43 732 757168-0
www.arrow.com/globalecs/at

Executive Insights

Christina Bäck
Channel Manager
Austria, Fortinet

Frau Bäck, Fortinet ist ein etablierter Anbieter im Bereich Cybersecurity. Was macht Ihre Plattform besonders?
Wir verfolgen einen ganzheitlichen Ansatz. Mit unserer Security Fabric verbinden wir alle Bereiche der IT-Sicherheit – vom Netzwerk über Cloud bis hin zu OT-Umgebungen. Das schafft Transparenz, reduziert Komplexität und ermöglicht automatisierte Reaktionen auf Bedrohungen. Entscheidend ist, dass alle Komponenten miteinander kommunizieren. So wird Sicherheit nicht als Produkt verstanden, sondern als fortlaufender Prozess.

Wie profitieren IT-Reseller konkret?
Unsere Partner erhalten ein flexibles Portfolio, das sich modular einsetzen und als Service anbieten lässt. Viele entwickeln darauf eigene Managed Services, was die Kundenbindung stärkt und planbare Erlöse schafft. Wir investieren stark in Ausbildung, weil Wissen im Channel der Schlüssel zu erfolgreicher Security ist.

Und für Techniker?
Techniker schätzen die zentrale Steuerbarkeit und Automatisierung. Ob Firewall, Cloud oder Endpoint – alles greift ineinander. Das reduziert Fehler und verschafft Zeit für strategische Aufgaben. Unsere Dashboards sind intuitiv und rollenbasiert, was die tägliche Arbeit deutlich erleichtert.

Was ist Ihre Vision für Fortinet?
Sicherheit soll kein Bremsklotz sein, sondern Innovation ermöglichen. Wir wollen Unternehmen unterstützen, Cybersecurity als strategischen Faktor zu sehen – für Wachstum und Nachhaltigkeit. Dabei setzen wir auf Technologie, aber auch auf Menschen: Unsere Partner und Teams machen den Unterschied. Denn trotz Automatisierung bleibt Sicherheit immer eine gemeinsame Aufgabe.

Advertorial

© KPMG

„Wir sind stolz darauf, die NATO zu unterstützen, und freuen uns darauf, der Allianz dabei zu helfen, von der KI-optimierten Oracle-Cloud in einer sicheren, widerstandsfähigen Umgebung zu profitieren.“

Robert Lamprecht,
Partner im Bereich IT Advisory bei KPMG

© upklyak/Freepik

WKO

EINFALLSTOR FÜR CYBERANGRIFFE

Cyberangriffe treffen zunehmend ganze Lieferketten. Laut der neuen KPMG-Studie „Cybersecurity in Österreich“ erfolgten 22 % der Datendiebstähle nicht beim Unternehmen selbst, sondern über externe Partner oder Dienstleister.

Unsere Wirtschaft ist zunehmend vernetzter, jedes Unternehmen hat Kunden und Lieferanten – entweder national oder auch international. Genau diese Lieferkette wird zunehmend zur Zielscheibe von Cyberangriffen. Bei 22 % der Unternehmen, die von Datendiebstahl betroffen waren, wurden die gestohlenen Informationen nicht direkt bei ihnen, sondern bei einem ihrer Dienstleister entwendet. Das geht aus der aktuellen Studie „Cybersecurity in Österreich“ mit Fokus auf Wien hervor. Heuer zum zehnten Mal erstellt von KPMG gemeinsam mit dem Kompetenzzentrum Sicheres Österreich (KSÖ).

Reale Bedrohung. 61 % der Befragten haben Bedenken, dass Angriffe gegen die Lieferanten oder Dienstleister Auswirkungen auf das eigene Unternehmen haben. „Das schwächste Glied in der Kette ist für Hacker natürlich das spannendste, das kann verheerende Konsequenzen für das Unternehmen haben und einen Dominoeffekt auslösen“, weiß Robert Lamprecht, Partner im Bereich IT Advisory bei KPMG. In vielen Fällen verschaffen sich Angreifer über den E-Mail-Account eines Mitarbeitenden Zugang zum internen System. Dort lesen sie zunächst unbemerkt mit, erweitern schrittweise ihre Zugriffsrechte auf firmeninterne Systeme, manipulieren Dokumente und schleusen Schadsoftware ein. Am Ende des Angriffs – etwa im Zuge eines Kaufprozesses – werden Zahlungsinformationen wie Kontodaten verändert, sodass das Geld auf ein fremdes Konto umgeleitet wird. „Cyberangriffe entlang der Lieferkette sind längst keine Ausnahme mehr, sondern eine reale Bedrohung für unsere Unternehmen – unabhängig von Größe oder Branche. Die aktuelle Studie zeigt deutlich, wie verwundbar externe Dienstleister sein können und welche Risiken daraus für die gesamte Wertschöpfung entstehen. Es braucht daher ein stärkeres Bewusstsein für Sicherheitsstandards in der Zusammenarbeit und klare Strategien, um auch die digitalen Schnittstellen zwischen Unternehmen resilient zu gestalten“, sagt Martin Heimhilcher, Obmann der Sparte Information und Consulting der WK Wien.

Wer steckt hinter Phishing & Co.? Ein Drittel der Cyberattacken hat seinen Ursprung in Europa. Cyberangriffe aus Asien haben seit dem letzten Jahr massiv zugenommen – von 6 % auf 26 % in diesem Jahr. Deutlich wurde auch, dass es eine Tendenz gibt, geistiges Eigentum zu stehlen. Um für die Zukunft gut aufgestellt zu sein, braucht es Zusammenarbeit – möglichst auf europäischer Ebene. 57 % der Befragten würden Security-Lösungen von österreichischen Unternehmen bevorzugen. „Es braucht eine europäische Sicherheitsarchitektur, die auch kleine und mittlere Unternehmen mitträgt. Dass über die Hälfte der Betriebe heimische Security-Lösungen bevorzugt, ist ein starkes Signal für den Standort Österreich – und eine Chance für unsere IT-Dienstleister“, so Heimhilcher abschließend. ▮

www.wko.at

Hornetsecurity

RANSOMWARE KEHRT ZURÜCK

Ransomware ist wieder auf dem Vormarsch: Laut dem neuen Report von Hornetsecurity war 2025 jedes vierte Unternehmen von einem Angriff betroffen. Während Cyberkriminelle neue Taktiken nutzen, sinkt gleichzeitig die Zahl der Firmen mit Versicherungsschutz.

Ransomware-Angriffe sind erstmals seit Jahren wieder auf dem Vormarsch. Laut der neuesten Forschungsergebnisse des Cybersecurity-Anbieters Hornetsecurity wurde ein Viertel der befragten Unternehmen 2025 Opfer eines Ransomware-Angriffs. Damit zeigt sich ein deutlicher Anstieg gegenüber 18,6 % im Jahr 2024. Diese Ergebnisse markieren damit das Ende eines mehrjährigen Rückgangs der Angriffe. Der Anstieg lässt sich auch darauf zurückführen, dass Cyberkriminelle ihre Methoden weiter diversifizieren und neue Technologien einsetzen, um Sicherheitsmaßnahmen zu umgehen. Während traditionelles Phishing nach wie vor der führende Angriffsvektor in fast der Hälfte der Angriffe ist, zeigt der Report, dass kompromittierte Endpunkte und gestohlene Zugangsdaten zunehmend als Zugangsvektor genutzt werden.

Wenig Absicherung. Während die Angriffe zunehmen, ist die Zahl der Organisationen, die in Ransomware-Versicherungen investieren, im Jahresvergleich gesunken. Aktuell verfügt weniger als die Hälfte aller Unternehmen über eine entsprechende Absicherung. Im Vorjahr lag dieser Wert noch bei 54,6 %. Daniel Hofmann, CEO von Hornetsecurity, sagt zu den Ergebnissen: „Es ist besorgniserregend, dass weniger Unternehmen in Ransomware-Versicherungen investieren, obwohl die Angriffe zunehmen. Allerdings ist zu beachten, dass es für Unternehmen heute schwieriger denn je geworden ist, eine Versicherung für solche Fälle abzuschließen. Angesichts der immer ausgefeilteren Taktiken von Hackern wird deutlich, dass Organisationen ihre Sicherheitsvorkehrungen konsequent ausbauen müssen, um diesen Attacken standzuhalten.“ Next-Gen-E-Mail-Sicherheitslösungen beispielsweise würden effektiv verhindern, dass Bedrohungen die Posteingänge erreichen, während Security-Awareness-Lösungen Endanwender:innen darin schulen, auch komplexe Angriffe wie Social Engineering zu erkennen. In Kombination mit unveränderbaren Backup-Lösungen entsteht so eine wirkungsvolle Strategie, um kritische Daten gegen Ransomware zu schützen. „Diese Maßnahmen erweisen sich als effektiv, unabhängig davon, ob ein Unternehmen gegen Ransomware versichert ist oder nicht“, Hofmann. ▮

www.hornetsecurity.com

© Freepik

secunet

Sichere VoIP-Telefonate

Der im nationalen Umfeld bereits bewährte, VS-NfD-zugelassene und nach Common Criteria EAL4+ zertifizierte secunet Session Border Controller (SBC) hat nun auch Zulassungen für den Einsatz in der NATO und der Europäischen Union erhalten. Im Kontext dieser multinationalen Organisationen können Behörden, Streitkräfte und Unternehmen ab jetzt Voice-over-IP (VoIP)-Netze sicher koppeln und anschließend als Nato Restricted und Restreint UE/EU Restricted eingestufte Informationen per VoIP-Telefonie und Videokonferenzen teilen. Der secunet SBC ermöglicht die sichere Kopplung und Anbindung von VoIP-Netzen mit verschiedenen Sicherheitseinstufungen – z. B. zwischen verschiedenen Standorten oder Organisationen.
Am Netzübergang leitet er VoIP-Anrufe weiter oder weist sie ab – je nachdem, ob die Sicherheitskriterien erfüllt sind. Auf diese Weise lassen sich abhörsichere Telefonate, Telefonkonferenzen oder auch Webkonferenzen per VoIP realisieren. Zudem überwacht die Lösung den VoIP-Verkehr und schützt so vor Angriffen. Um VoIP-Telefonate mit eingestuften Inhalten führen zu können, sind zusätzlich zum secunet SBC auch Endgeräte mit entsprechender Zulassung erforderlich.

www.secunet.com

Fortinet

ZWISCHEN FIREWALL UND VERANTWORTUNG

© Freepik

Christina Bäck, Head of Channel Management Austria bei Fortinet, spricht mit uns über ganzheitliche Sicherheit, die Bedeutung starker Partner im Channel, den richtigen Umgang mit Cloud und KI. Und warum trotz Automatisierung der Mensch unverzichtbar bleibt.

EHZaustria: ***Was wünschen Sie sich von Unternehmern, die plötzlich feststellen: „Da war doch etwas mit Security“?***
Christina Bäck: Grundsätzlich einmal Aufgeschlossenheit und das Bewusstsein, dass Security wichtig ist. Und dass sie nicht nur ein technologisches Thema ist, sondern bis in die Geschäftsführungsebene reicht. Es gibt mittlerweile viele Regulatorien und gesetzliche Vorschriften im Bereich Security, und da ist es wichtig, offen zu sein und zu verstehen, dass es nicht mehr reicht, einzelne Technologien oder Produkte einzusetzen. Security muss ganzheitlich gedacht werden. Wir sagen gerne: Think big, act small.

Wir reden alle sehr viel über Security, aber ist das nicht manchmal ein Blasen-Denken?
Bäck: Ich glaube, solange man selbst keine direkte Erfahrung gemacht hat oder nicht mit einer Bedrohung in Berührung gekommen ist, bleibt das Thema sehr abstrakt. Cybergefahren sind ja unsichtbar, man kann sie nicht greifen. Viele denken: „Ja, das ist schlimm, aber mir passiert das nicht. Bei mir gibt’s ja nichts zu holen.“ Dieses Denken ist gerade bei kleineren und mittleren Unternehmen noch sehr verbreitet. Erst wenn man selbst oder jemand im Umfeld betroffen ist, ein befreundetes Unternehmen oder ein Geschäftspartner, dann setzt ein Umdenken ein.

Wie findet man die richtige Lösung, die möglichst alles abdeckt? Kann das ein Hersteller alleine leisten?
Bäck: Das ist zumindest unser Anspruch. Die hundertprozentige Sicherheit wird es nie geben, aber wir sehen uns als einen der Anbieter, der diesem Ideal am nächsten kommt. Viele Unternehmen sind überfordert, wenn sie verstehen, dass Cybersecurity nicht nur aus einer Firewall oder einer Endpoint Protection besteht. Genau hier braucht es Partner, die das große Ganze verstehen und Sicherheit ganzheitlich denken. Und das ist einer der Gründe, warum unsere Reseller gerne mit uns arbeiten. Sie können mit uns nicht nur ein einzelnes Produkt verkaufen, sondern in die Breite wachsen und ein ganzheitliches Security-Angebot machen. Dazu setzen wir stark auf laufende Weiterbildung, mit Webinaren, Tech-Schulungen und Programmen gemeinsam mit unseren Distributoren.

Fortinet nutzt KI, um Sicherheitsprodukte zu verbessern. Wie sieht das konkret aus?
Bäck: Machine Learning ist bei uns schon seit vielen Jahren fester Bestandteil unserer Produkte. Hier ist KI schon lange unverzichtbar. In den letzten Jahren kam dann GenAI dazu. Wir integrieren KI-basierte Assistenten direkt in unsere Produkte, um etwa die Arbeit unserer Systemtechniker zu erleichtern. Unsere Partner haben dann besondere Freude, wenn die KI etwa die Dokumentation von Vorfällen übernimmt, also automatisch Incident-Daten sammelt, Threat-Analysen erstellt und daraus eine verständliche Management Summary generiert. Wichtig aber: Es gibt nicht das eine KI-Produkt bei Fortinet. KI ist in unser gesamtes Portfolio eingebettet und wird dort laufend weiterentwickelt.

Viele Unternehmen glauben, dass ihre Daten in der Cloud automatisch sicher sind.
Bäck: Das ist ein weit verbreiteter Irrglaube. Viele gehen davon aus, dass mit dem Schritt in die Cloud auch automatisch für ausreichend Sicherheit gesorgt ist. Aber so ist es nicht. Der Cloud-Provider stellt die Infrastruktur und gewisse Basis-Security-Funktionen bereit – mehr aber auch nicht. Alles, was darüber hinausgeht, also die Sicherheit von Applikationen, Daten und der gesamten Konnektivität, liegt weiterhin in der Verantwortung desjenigen, der die Services nutzt.

Welche strategischen Schwerpunkte setzt Fortinet in den kommenden Monaten?
Bäck: Ganz klar im Bereich Dienste. Wir sehen, dass Security zunehmend als Service bereitgestellt werden muss – also im Sinne von Security-as-a-Service. Hardware und Edge bleiben weiterhin wichtig, und das ist auch ein Bereich, in dem wir sehr stark sind. Aber entscheidend ist die Kombination mit Cloud-basierten Services, die als All-in-One-Support-Paket in einem flexiblen Consumption-Modell verfügbar sind. Ein weiterer Schwerpunkt liegt auf dem Thema SOC – Security Operations Center. Es geht nicht nur darum, Angriffe abzuwehren, sondern auch darum, wie man reagiert, wenn etwas passiert. In diesem Bereich sehen wir derzeit eine besonders starke Entwicklung und investieren gezielt in entsprechende Strategien.

Welche Rolle spielt der Channel für Fortinet?
Bäck: Wir entwickeln Technologien und bieten Services an. Dabei setzen wir auf unsere Reseller, Systemhäuser und Partner, um das, was wir entwickeln, zu über einer halben Million Endkunden weltweit zu bringen. In den letzten Jahren haben wir auch massiv in Channel Education investiert und eigene Programme aufgebaut, um den Channel in der Breite zu stärken, damit er unsere Technologien auch optimal beim Kunden einsetzen kann. Security verändert sich permanent. Was gestern aktuell war, ist heute schon überholt. Die Geschwindigkeit der Entwicklung ist enorm, und genau deshalb muss man das Ganze laufend orchestrieren und weiterentwickeln.

„Die hundertprozentige Sicherheit wird es nie geben, aber wir sehen uns als einen der Anbieter, der diesem Ideal am nächsten kommt.“
Christina Bäck,
Head of Channel Management Austria bei Fortinet

© Fortinet

Haben Sie Wünsche oder Erwartungen an die Zusammenarbeit mit der Distribution?
Bäck: Wir haben wirklich sehr gute Distributoren, die unsere Vision mittragen und aktiv unterstützen, das breite Fortinet-Portfolio im Channel zu etablieren. Mein Wunsch ist, dass dieses Bewusstsein und der Mehrwert unserer Plattform noch stärker hervorgehoben werden – über alle Resellergrößen hinweg. Wichtig ist auch, gemeinsam Managed Services aufzubauen, also Lösungen, bei denen unsere Technologie ein Teil des Gesamtangebots ist und ein klarer Mehrwert rundherum entsteht. Dafür brauchen wir die Distribution als Multiplikator.

Was ist Ihnen persönlich in Ihrer Arbeit besonders wichtig?
Bäck: Uns ist ganz wichtig, dass wir Fortinet ein Gesicht geben. Der Großteil unserer Partner hat uns schon einmal live auf Events gesehen, wir touren regelmäßig durch ganz Österreich. Wir verkaufen nicht nur Technologie. Business wird am Ende des Tages zwischen Menschen gemacht. Bei aller KI und bei aller Automatisierung: Der menschliche Aspekt darf nicht verloren gehen.

www.fortinet.com

Onekey

SICHER DANK SBOM

© Freepik

Mit dem Cyber Resilience Act verpflichtet die EU Hersteller digitaler Produkte zur Offenlegung aller Software-Komponenten. Onekey unterstützt Unternehmen mit „angereicherten SBOMs“, die nicht nur Transparenz, sondern auch geprüfte Sicherheit bieten.

Die EU-Verordnung Cyber Resilience Act (CRA) schreibt vor, dass die Hersteller und Inverkehrbringer digitaler Produkte mit Internetanschluss künftig eine Software Bill of Materials (SBOM), also eine Software-Stückliste, vorweisen müssen. Ziel ist es, mögliche Software-Schwachstellen, die Hackern als Angriffsfläche dienen könnten, zu identifizieren, um sie zeitnah beheben zu können. Der CRA verlangt daher für vernetzte Geräte, Maschinen und Anlagen ausnahmslos eine detaillierte Auflistung aller Programme, Bibliotheken, Frameworks und Abhängigkeiten mit genauen Versionsnummern der einzelnen Komponenten, Informationen zu den jeweiligen Lizenzen, Angaben zu den Urhebern und einem Überblick über alle bekannten Schwachstellen und Sicherheitslücken. Diese Anforderungen zu erfüllen fällt vielen Herstellern schwer, und sei es nur, weil sie von ihren Vorlieferanten nicht die gewünschten Informationen in der notwendigen Vollständigkeit erhalten. Aus diesem Grund sind viele SBOMs unvollständig, veraltet oder ohne Kontext zu Schwachstellen. Für die in der EU-Regulatorik zwingend vorgeschriebene Nachweispflicht von Seiten der Hersteller sind diese lückenhaften und teilweise überholten Software-Stücklisten unbrauchbar.

Sicherheitspass. Jetzt hat das Cybersicherheitsunternehmen Onekey seine Plattform zur Überprüfung von Gerätesoftware auf Sicherheitsmängel mit einer neuen Funktion versehen, um sog. angereicherte SBOMs zu erzeugen. Die stark erweiterten Software-Stücklisten enthalten alle relevanten Informationen zu Schwachstellen. Die damit erzeugten SBOMs erfüllen alle Anforderungen der Branche. Sie enthalten nicht nur die Schwachstellen mit Risikoeinordnung, sondern stellen auch die Nachweise und Begründungen in einer einzigen leicht handhabbaren Datei bereit. „Somit wird die SBOM von der bloßen Stückliste zu einer Art Sicherheitspass mit integrierter Risikobewertung“, erklärt Jan Wendenburg, CEO von Onekey. Er weiß aus vielen Gesprächen mit Herstellern: „Die häufig komplexen Lieferketten und das oftmals mangelnde Verständnis von Lieferanten außerhalb der Europäischen Union für EU-spezifische Regulierungen erschweren es, den Anforderungen des Cyber Resilience Act nachzukommen.“ Die neue Funktionalität stellt einen entscheidenden Beitrag dar, diese Hürde zu überwinden, heißt es bei Onekey.

www.onekey.com

Sophos

Ganzheitlich statt punktuell

Der Endpoint ist oft die erste und beste Gelegenheit, Angriffe zu stoppen. Und moderne Endpoint Protection geht weit über die bloße Abwehr einzelner Bedrohungen hinaus. Entscheidende Differenzierungsmerkmale liegen in der Datenqualität der Telemetrie, der Architektur und der Integrationsfähigkeit der Sicherheitsplattform. Moderne Sicherheitsplattformen wie Sophos XDR (Extended Detection and Response) nutzen KI-gestützte Workflows, umfassende Integrationen und eine einheitliche Sicht auf die gesamte IT-Infrastruktur, um Bedrohungen effizient zu identifizieren und darauf zu reagieren. „Die Zeiten, in denen einzelne Sicherheitsprodukte ausgereicht haben, sind vorbei. Cyber-Resilienz entsteht heute durch eine ganzheitliche, lernfähige Plattformarchitektur, die Prävention, Erkennung und Reaktion intelligent verbindet“, sagt Michael Veit, Security-Experte bei Sophos. „Unternehmen, die ihre Sicherheit dynamisch orchestrieren, reagieren schneller und können Angriffe stoppen, bevor sie Schaden anrichten.“

Eine moderne Sicherheitsarchitektur ermöglicht es, diesen Schutz auf E-Mail, Netzwerk, Cloud und Identität auszuweiten. So entsteht eine durchgängige Detection & Response-Strategie, die eine Ausbreitung verhindert und kritische Systeme schützt. Damit sinken Risiken, verkürzen sich Erkennungszeiten und werden Reaktionen schneller.

www.sophos.de

Ultimo ernennt neuen Senior VP

Ultimo, Anbieter von Software im Bereich Enterprise Asset Management, hat **Philip Neal** zum neuen Senior Vice President für die Regionen EMEA und APAC ernannt. Neal war zuvor Senior Area Vice President und Head of Industrial in Großbritannien und Irland bei Salesforce. Er bringt jahrzehntelange Erfahrung mit Enterprise-Technologien mit und hat die digitale Transformation in verschiedenen Branchen erfolgreich mitgestaltet.

Pure Storage ernennt CRO

Pure Storage, gab Anfang November die Ernennung von **Patrick Finn** zum Chief Revenue Officer bekannt. Finn hat die Leitung des globalen Vertriebs und der Vertriebskanäle übernommen. Er folgt auf Dan FitzSimons, der dem Unternehmen weiterhin beratend zur Seite stehen wird. Finn verfügt über mehr als drei Jahrzehnte Erfahrung im Vertrieb und in Führungspositionen im privaten und öffentlichen Sektor.

Team Lead Strategic Partnerships für Myra

Myra Security ernennt **Amer Buljubasic** zum Team Lead Strategic Partnerships. In dieser Position zeichnet er für den Ausbau und die Weiterentwicklung der internationalen Partnerschaften verantwortlich. Buljubasic bringt mehr als 15 Jahre Erfahrung im Channel und umfassende Expertise im Aufbau internationaler Partnerprogramme mit. „Ich war schon immer ein Verfechter einer Channel-First-Strategie“, erklärt er.

Verstärkung für Geschäftsführung

Mit umfassender Erfahrung im europäischen Technologiesektor ist **Stéphane Israël** im Oktober 2025 zu Amazon Web Services (AWS) gestoßen. Als Geschäftsführer der AWS European Sovereign Cloud wird er die globalen Bemühungen des Unternehmens im Bereich digitaler Souveränität vorantreiben. „Ich freue mich, zu einem entscheidenden Zeitpunkt für die digitale Souveränität in Europa und weltweit zu AWS zu stoßen“, erklärt er.

Neuer CFO/ COO für Infinigate

Die Infinigate Group ernennt **Peter Meier** zu ihrem neuen Chief Financial Officer (CFO) sowie Chief Operating Officer (COO). Meier bringt langjährige Erfahrung als CFO und Vorstandsmitglied globaler Technologieunternehmen mit, wo er erfolgreich die operative Geschäftstransformation geleitet hat. Bei Infinigate wird er die Finanzabteilung leiten, die Finanzanlagen von Infinigate optimieren und die M&A-Agenda unterstützen.

Eset verstärkt Vertriebsteam

Der europäische IT-Sicherheitshersteller Eset verstärkt ab sofort sein DACH-Vertriebsteam mit **Axel Witt** als Senior Channel Account Manager. Der Vertriebsexperte bringt über 20 Jahre an Erfahrung aus der IT- und Retail-Branche mit. Zuvor durchlief er unterschiedliche Positionen beim Distributor Ingram Micro und bei Kaspersky, wo er zuletzt in den vergangenen 18 Jahren den Retail- bzw. Consumer-Bereich verantwortete.

Neuausrichtung des Führungsteams

© Verena Amann/LinkedIn

Verena Amann

Die accompio Gruppe stellt ihr Führungsteam neu auf. Die Geschäftsführung wurde mit 1. November durch eine neu geschaffene Geschäftsführungsposition ergänzt. Neben den Geschäftsführern Dr. Christian Böing (CEO) und Georg Willig (CFO), wird künftig Verena Amann als Geschäftsführerin und Chief People Officer (CPO) die Verantwortung für das Personalwesen der gesamten accompio Gruppe übernehmen. Amann wird damit zentral die Themenbereiche People, Talent-Management, Recruiting, Unternehmenskultur und Personalstrategie steuern, um die accompio Gruppe noch stärker als attraktiven Arbeitgeber im Markt zu positionieren.

Dr. Andreas Herch hat die operative Führung der Business „Unit accompio“ Enterprise übernommen. Unter seiner Verantwortung soll accompio Enterprise weiter mit Großkunden wachsen. Das Segment „accompio MidMarket“ wird Tim Körner als CEO führen. Er wird die Position als Managed-Service-Partner für KMU weiter ausbauen. Zusätzlich wird Ruben Mosblech als neuer Verantwortlicher für das Group Marketing arbeiten.

www.accompio.com

EHZ austria

© Creativeart/Freepik

Veeam Österreich

DIE LETZTE RETTUNG

Backup ist längst mehr als Datensicherung. Es ist der letzte Rettungsanker in Zeiten, in denen Angriffe unvermeidbar sind. Im Interview erklärt Mario Zimmermann, Country Manager von Veeam Österreich, warum Resilienz, KI und Cloud die Zukunft der Datensicherheit bestimmen.

EHZaustria: ***Ist ein Backup die letzte Rettung?***
Mario Zimmermann: Wir gehen aktuell mit genau diesem Thema nach draußen: Backup als der letzte Rettungsanker. Die Frage lautet ja heute nicht mehr ob, sondern wann etwas passiert. Und dann stellt sich die entscheidende Frage: Was dann? Geht man davon aus, dass ein Angriff oder ein Ausfall eintreten kann, ist entscheidend, wie man darauf reagiert. Genau hier kommt das Thema Backup ins Spiel. In einem ganzheitlichen Sicherheitskonzept ist es daher ein zentraler, strategischer Bestandteil. Kurz gesagt: Ja – Backup ist die letzte Rettung.

Was ist Ihre Empfehlung für ein gutes Backup-Konzept?
Zimmermann: Wir orientieren uns an der 3-2-1-Regel, die inzwischen um 1 und 0 erweitert wurde. Das bedeutet: Es sollten mindestens drei Kopien der Daten existieren, auf zwei unterschiedlichen Speichermedien, und eine davon sollte extern oder offline gesichert sein. Die zusätzliche 1 steht für „immutable", also unveränderbare Daten. Hier kommen sowohl Veeam- als auch Storage-Technologien ins Spiel. Viele S3-Storage-Anbieter stellen sicher, dass Backups nicht verändert, verschlüsselt oder gelöscht werden können. Und die 0 steht für null Fehler nach der Überprüfung der Backups. Wenn man diese 3-2-1-1-0-Regel konsequent einhält, ist man auf der sicheren Seite.

Man hört immer wieder, dass auch Backups Ziel von Angriffen sind. Dann spielt man im Ernstfall wieder kompromittierte Daten zurück.
Zimmermann: Laut unserem aktuellem Ransomware Trends Report werden in 89 % der Angriffe zuerst Backup-Umgebungen ins Visier genommen, in etwa 34 % der Fälle gelingt es Angreifern, Backups zu verändern oder ihre Position auszubauen. Daher muss sich jedes Unternehmen die Fragen stellen: Bin ich technisch korrekt aufgestellt? Habe ich die richtigen Schutztechnologien und aktuelle Patches? Sind Mitarbeitende geschult, damit Angreifer keine Zugangsdaten erhalten? Wenn ein Angreifer einmal erfolgreich war – und gegebenenfalls bezahlt wurde – ist die Wahrscheinlichkeit hoch, dass er wiederkommt. Deshalb sind vorbeugende Maßnahmen und eine ganzheitliche Resilienzstrategie so wichtig.

Spielt KI beim Thema Backup eine Rolle?
Zimmermann: Ohne KI wird es künftig nicht gehen. Gerade in Zeiten des Fachkräftemangels brauchen wir Technologien, die automatisieren und uns unterstützen. KI ist längst Realität und sie wird vieles übernehmen. Dabei müssen wir uns bewusst sein: KI steht nicht nur uns, sondern auch Angreifern zur Verfügung. Dadurch werden Attacken komplexer und deutlich schneller. Früher dauerte ein Angriff Wochen oder Monate, heute kann vom Eindringen bis zur Verschlüsselung alles innerhalb von 24 Stunden passieren. KI sorgt also für extreme Beschleunigung und Skalierbarkeit – auf beiden Seiten. Wir haben im Oktober Securiti AI in unser Portfolio aufgenommen. Früher war es uns egal, welcher Datensatz gesichert wurde. Jetzt analysieren wir die Daten zusätzlich. Wir überwachen Datenströme, klassifizieren sensible Informationen, prüfen Zugriffsrechte und sichern gezielt kritische Inhalte.

Sie haben das Thema Resilienz bereits angesprochen. Was verstehen Sie konkret darunter?
Zimmermann: Wir sprechen heute in der gesamten Branche nicht mehr nur über Backup oder Wiederherstellung, sondern über Data Resilience, also die Frage: Nicht ob, sondern wann – und was dann? Veeam sieht Resilienz als Zusammenspiel aus fünf Säulen: Backup und Recovery, Data Portability, Security, Intelligence und Continuity. Daten wandern vom Notebook über den Server bis in die Cloud und unsere Lösungen müssen diesen Daten nahtlos folgen. Gleichzeitig bauen wir immer mehr Sicherheitsfunktionen ein, weil Backups mittlerweile Target Number One sind. Mit der Integration von Securiti AI schließen wir hier den Kreis und setzen zusätzlich auf KI, um Anomalien schneller zu erkennen und entsprechend zu reagieren. Um das Thema messbar zu machen, haben wir gemeinsam mit dem MIT, McKinsey, Microsoft und anderen Branchengrößen das Data Resilience Maturity Model entwickelt. Es ermöglicht Unternehmen, ihre eigene Widerstandsfähigkeit zu bewerten und zu verbessern. Das Ergebnis der ersten Auswertungen war ernüchternd: 70 % der Befragten glauben, resilient zu sein, tatsächlich sind es aber nur 8 %. Dieser Gap zwischen Wahrnehmung und Realität zeigt sich auch in Österreich. Gründe dafür sind Fachkräftemangel, Überlastung und unvollständig genutzte Technologien. Mit dem Maturity Model geben wir Unternehmen ein Werkzeug an die Hand, um genau das zu ändern: Es bewertet Technologie, Prozesse und Menschen gleichermaßen und zeigt, wo man steht. Und wie man Schritt für Schritt resilienter wird.

Welche Rolle spielt die Cloud in Ihrer Strategie?
Zimmermann: Die Cloud – genauer gesagt die Data Cloud – steht aktuell ganz klar im Fokus vieler Unternehmen. Wir haben vor rund zwei Jahren die Veeam Data Cloud auf den Markt gebracht, über die wir Backup-as-a-Service anbieten. Das bedeutet: Unternehmen müssen sich nicht mehr um Management, Installationen oder Security-Updates kümmern. All das passiert zentralisiert. Mit Services wie Backup für Microsoft 365 oder Entra ID können wir Backups direkt in einer Microsoft Cloud oder in einem Veeam Tenant speichern. Das nennen wir Veeam Vault. Dort sind die Daten geschützt, gehärtet und unveränderbar abgelegt. Damit lassen sich Daten sicher auslagern und gleichzeitig Compliance-Anforderungen erfüllen. Unser Fokus liegt klar auf dieser Weiterentwicklung, aber wir bieten auch Wahlfreiheit. Mit der Veeam Data Platform können Unternehmen ihre Umgebung selbst betreiben. Oder sie entscheiden sich für die Veeam Data Cloud, wenn Cloud-first ohnehin ihre Strategie ist. Wichtig ist: Nicht wir entscheiden, was „state of the art" ist, sondern jedes Unternehmen selbst.

Wie wichtig ist der Channel für Veeam?
Zimmermann: Der Channel ist und bleibt unser Fundament. Wir kommen aus dem Channel und wir bleiben im Channel. Auch unsere Veeam Data Cloud ist keine Direktlösung für Endkunden, sondern wird ausschließlich über Partner und Distributoren wie etwa Arrow und TD Synnex angeboten. Wir verfügen über eine große Partnerlandschaft und legen großen Wert darauf, sie regelmäßig zu schulen. Die Themen werden zunehmend komplexer. Früher war Backup und Restore das Kerngeschäft, heute geht es um Security, Multi-Cloud, Härtung und Resilienz. Das ist auch für Partner eine Herausforderung, da sie viele Hersteller im Portfolio haben. Gerade hier kann die Cloud-Strategie helfen. Sie nimmt viele technische Aufgaben ab und stellt sicher, dass Sicherheitsstandards eingehalten werden. Alle unsere Cloud-Services und Lösungen werden weiterhin ausschließlich über Partner angeboten. Das ist und bleibt unser klares Commitment gegenüber dem Channel. ▮

www.veeam.com

„Laut unserem aktuellem Ransomware Trends Report werden in 89 % der Angriffe zuerst Backup-Umgebungen ins Visier genommen."

Mario Zimmermann,
Country Manager von Veeam Österreich

© Veeam Software

© NetApp

„KI unterstützt über unser gesamtes Produkt-Portfolio die Nutzer mit verschiedensten Möglichkeiten in der Business-Telefonie.“

Christian Sitz,
Manager Solutions Engineering

NetApp

Neue Funktionen

NetApp hat neue Cyberresilienz-Funktionen angekündigt. Der erweiterte Ransomware Resilience Service soll Kund:innen dabei unterstützen, ihre Dateninfrastruktur zu einem zentralen Bestandteil ihrer Sicherheitsstrategie zu machen. Der Service integriert KI-gestützte Ransomware-Erkennung sowie zwei neue Funktionen. Diese erlauben es Unternehmen erstmals, Datenverletzungen in Enterprise-Storage-Umgebungen zu erkennen und unternehmenskritische Daten mithilfe isolierter Recovery-Umgebungen sicher wiederherzustellen. „Unternehmen müssen so schnell wie möglich wissen, was bei einem Cyberangriff passiert ist, um ihre Daten effektiv zu schützen und entsprechende Maßnahmen zu ergreifen“, sagt Christian Sitz, Manager Solutions Engineering bei NetApp Austria GmbH. „Unsere neuen KI-gestützten Funktionen können bereits die ersten Anzeichen potenzieller Versuche von Datendiebstahl identifizieren. Dadurch erweitern sie unsere bestehenden Funktionen zur Erkennung von Ransomware-Angriffen auf strukturierte sowie unstrukturierte Daten. Der Storage bildet damit die letzte Verteidigungsinstanz, um die wertvollen Daten unserer Kunden zu schützen. Deshalb entwickeln wir den sichersten Storage der Welt kontinuierlich weiter.“

www.netapp.com

Acronis

SICHER UND EINFACH

Mit True Image 2026 bringt Acronis eine rundum erneuerte All-in-one-Lösung für Backup und Cyberschutz auf den Markt. Dank KI-basierter Bedrohungserkennung, integriertem Patch-Management und einfacher Bedienung schützt die Software Privatanwender:innen zuverlässig.

True Image 2026 heißt die neue Version der nativ integrierten Backup- und Sicherheitssoftware von Acronis für Privatanwender:innen. Sie verfügt über ein integriertes Patch-Management für Windows, das vollständig automatisierte Hintergrund-Updates ermöglicht, sowie eine verbesserte Sicherheits-Engine, die KI-basierte Module für Bedrohungserkennung, Ransomware-Schutz und Malware-Scans umfasst. Sie schützt proaktiv auch vor bisher unbekannten Cyberbedrohungen und hilft dabei, Schwachstellen zu schließen und Angriffe abzuwehren. Ihre Integration zeigt, wie Acronis seine Lösungen kontinuierlich verbessert, um Nutzer:innen vor zunehmend komplexen Cyberbedrohungen zu schützen. Die All-in-one-Lösung vereinfacht komplexen Schutz mit einer benutzerfreundlichen App und vereint schnelle Backups, eine einfache Wiederherstellung, erweiterten Cyberschutz sowie Identitätsschutz (bisher nur in den USA verfügbar). Mit der Lösung können bis zu fünf Computer sowie eine unbegrenzte Anzahl mobiler Geräte umfassend und zuverlässig geschützt werden.

All-in-one-Lösung schützt. Angesichts der Zunahme von Ransomware und Identitätsdiebstahl sowie der sich ständig weiterentwickelnden Cyberrisiken benötigen Nutzer:innen mehr als nur Backups. „Acronis True Image 2026 wurde für alle entwickelt, die keine Zeit haben, sich um ihre digitale Sicherheit zu sorgen“, so Gaidar Magdanurov, President von Acronis. „Die meisten Menschen wollen sich nicht mit Backups und Sicherheit befassen, sondern die Gewissheit haben, dass sie gut geschützt sind. Mit Acronis True Image 2026 haben wir diesen Schutz automatisiert. Anstatt für zwei separate Programme zu bezahlen und mehrere Abonnements zu verwalten, können sich Nutzer:innen auf ein einziges Tool verlassen, mit dem sie im Durchschnitt bis zu 55 % an Kosten einsparen.“ Die Lösung bietet zudem grundlegende Funktionen wie KI-basierte Bedrohungserkennung zum Schutz vor Ransomware, Malware und anderen komplexen Angriffen. Über klassische Backup-Funktionen hinaus ermöglicht die Lösung eine schnelle Wiederherstellung und sicheres Klonen von Laufwerken. Mithilfe der intuitiven Benutzeroberfläche können Nutzer:innen ihr digitales Leben mit einem einzigen Klick sichern, wiederherstellen und schützen.

www.acronis.com

© rawpixel.com/Freepik

© Stockking/Freepik

© HYCU

Andy Fernandez,
Director of Product Management
bei HYCU

HYCU

SECHS STILLE KILLER

Cloud-Backups gelten als sichere und komfortable Lösung für den Schutz sensibler Daten. Doch in der Praxis zeigt sich: Hinter der einfachen Fassade lauern technische Hürden, versteckte Kosten und Risiken, die IT-Teams zunehmend vor große Herausforderungen stellen.

Cloud-Backups gelten als einfache und bequeme Lösung, um Daten und Anwendungen zu schützen. Doch der Schein trügt. Laut Andy Fernandez, Director of Product Management bei HYCU, gibt es sechs „stille Killer“, die die Performance solcher Backups untergraben. Statt der lange propagierten „einzigen Schnittstelle“ jonglieren Unternehmen heute mit zahlreichen Konsolen für verschiedene Dienste – ein wachsendes Konsolenchaos, das die Komplexität erheblich erhöht. Hinzu kommt ein Automatisierungswildwuchs: In Multi-Cloud-Umgebungen müssen IT-Teams unzählige APIs manuell verknüpfen, um grundlegende Sicherheitsfunktionen zu gewährleisten. Doch selbst dann bleiben blinde Flecken in der Datenbank, da viele Cloud-Dienste keine adäquate Backup-Unterstützung bieten und das ausgerechnet dort, wo oft die geschäftskritischsten Informationen liegen.

Ein weiteres Problem ist die Egress-Kostenfalle. Während Speicherung in der Cloud günstig erscheint, entstehen beim Verschieben oder Wiederherstellen von Daten schnell hohe Kosten, die Multi-Cloud-Strategien unwirtschaftlich machen. Dazu kommt die Speicherüberlastung – ineffiziente Backups ohne Deduplizierung treiben die Kosten kontinuierlich in die Höhe. Und selbst wenn alles gesichert scheint, lauert die letzte Hürde: Hindernisse bei der Wiederherstellung. Granulare Restores sind oft schwierig, Disaster-Recovery-Optionen begrenzt, und das Abrufen archivierter Daten kann ein Vielfaches der Speicherkosten verursachen. Für das Management bleiben diese Risiken meist unsichtbar. Für die IT-Teams sind sie tägliche Realität.

Die DIY-Falle. Viele setzen auf selbst gebaute Backup-Lösungen mit Scripts, Workflows und Automatisierungen, die ständig gewartet werden müssen. So entsteht eine komplexe Rube-Goldberg-Maschine ohne Garantie für Wiederherstellung oder Compliance. Unternehmen wollen weder acht verschiedene Backup-Produkte noch ein einziges, das stark angepasst wurde, denn die versteckten Kosten aus Zeit, Energie und verlorener Fokussierung summieren sich. Mit wachsender Nutzung von KI und verteiltem Data Warehousing bremsen solche Eigenkonstruktionen zunehmend. Diese stillen Killer erscheinen selten in Vorstandsberichten, sind für IT-Teams jedoch tägliche Realität.

www.hycu.com

„Mit DPX 4.13 setzen wir neue Maßstäbe in Sachen Zuverlässigkeit von Backups und Cyber-Resilienz.“

Ryan Kaw,
Vice President of Sales bei
Catalogic Software

Catalogic Software

Neue Version

Catalogic Software hat seine neueste Version seiner All-in-One-Lösung für die Sicherung und Wiederherstellung von Unternehmensdaten namens Catalogic DPX 4.13 vorgestellt. Die meisten Backup-Produkte erfordern eine Kombination verschiedener Anbieter für Software, Speicher und Ransomware-Schutz. Das führt zu mehr Komplexität und somit mehr Fehlerquellen. DPX bietet alles in einer einheitlichen, softwaredefinierten Plattform, die auf der vorhandenen Hardware eines Unternehmens läuft. DPX wurde entwickelt, um vor allem zu schützen – von versehentlichem Löschen bis hin zu Ransomware. Damit wird jedes Backup unveränderlich, verschlüsselt, verifiziert und ist für eine saubere Wiederherstellung bereit.

Einzige Plattform. DPX 4.13 bietet wichtige Neuerungen wie automatisierte Integritätsprüfungen von Backups, proaktive Malware-Scans, Auswahl von Wiederherstellungspunkten und nahtlose Netzwerkkonfiguration. Damit können Unternehmen über eine einzige Plattform die Wiederherstellbarkeit überprüfen, ihre Cyber-Resilienz stärken und Disaster-Recovery-Prozesse optimieren. „Mit DPX 4.13 setzen wir neue Maßstäbe in Sachen Zuverlässigkeit von Backups und Cyber-Resilienz“, so Ryan Kaw, Vice President of Sales bei Catalogic Software. „Dank dieser neuen Funktionen können Kunden darauf vertrauen, dass ihre Backups wiederherstellbar, sicher und flexibel genug sind, um den komplexen Wiederherstellungsszenarien von heute gerecht zu werden.“

http://catalogicsoftware.com/de

© Concept International

Smartes Desk-Sharing

Der Qbic TDD-1000 ist ein Smart-Office-Gerät für hybride Arbeit und New Work. Die erweiterte Dockingstation für zwei 4K-Bildschirme mit kleinem, lichtsensorgesteuertem Touchscreen und AndroidOS ist ein cleverer Helfer, der Schreibtischbuchung, Ressourcenmanagement und Arbeitsplatztechnik in einem Gerät vereint.
Das NFC-fähige Terminal lädt ein angestecktes Notebook mit bis zu 100W PD und ist in drei Varianten verfügbar: mit optionalem 15-Watt Wireless-Charger, einem Long-Range- oder einem Apple-kompatiblen NFC-Reader. So kann der Log-In Transponder in der Tasche bleiben oder das iPhone dient zur Arbeitszeiterfassung.

Schnell und flexibel. Das Qbic TDD-1000 wird wie eine einfache Dockingstation auf den Schreibtisch gestellt und ist schnell mit Strom und Monitoren verbunden und damit flexibel einsatzfähig.
Es nimmt mit seinen kompakten Ausmaßen (21,5 x 16,3 cm) nur den Platz eines halben DIN A 5-Blocks ein. Das integrierte 3,9-Zoll-Direct-Bonding-Touchdisplay zeigt übersichtlich die gewünschte Android App an und lässt sich per Touch, NFC-Tag oder Smartphone/Rechner bedienen. Das 3,9-Zoll-Touchdisplay leuchtet mit maximal 400 Nits, also etwas heller als ein üblicher Office-Monitor. Da kann auch einmal Sonne ins Büro scheinen. Das TDD-1000 ist aber nicht nur ein Android-Terminal mit vielfältigsten App-Möglichkeiten, es ist auch ein vollwertiger USB-C-Hub mit Schnellladefunktion.

www.qbictechnology.com

© Lexar

Lexar

MOBIL UND MAGNETISCH

Speziell für Content-Ersteller sowie Videografen und Fotografen hat Lexar die tragbare, magnetische SSD ES5 entwickelt.

Sie bietet Lese- und Schreibgeschwindigkeiten von bis zu 2000 MB/s für schnelle Dateiübertragungen und einen reibungslosen Arbeitsablauf. Dank der integrierten MagSafe-Kompatibilität lässt sie sich einfach an verschiedene Smartphones, wie iPhone 15 Pro/Pro Max, iPhone 16 Pro/Max und Samsung S25, anschließen. Sie unterstützt Apple ProRes-Aufnahmen mit 4K bei 60/120 FPS und Samsung Pro Video mit 8K bei 30 FPS1, sodass Kreative die internen Speicherbeschränkungen umgehen und konstant hohe Qualität direkt auf der SSD aufnehmen können.

Einfache Erweiterung. Zudem lässt sich der Speicher des Smartphones mit der Lexar App, die mit allen tragbaren SSDs von Lexar kompatibel ist und sowohl mit iOS- als auch mit Android-Geräten funktioniert, durch automatische Foto- und Videosicherungen ganz einfach erweitern.
Durch die IP65-Zertifizierung ist die SSD staub- und wasserdicht. Darüber hinaus wurde sie auf Stürze aus bis zu drei Metern Höhe getestet. Das robuste Silikondesign umfasst einen Kabelorganisator, der gleichzeitig als Trageband dient. Es lässt sich mithilfe der magnetischen Halteplatte nahtlos an einem MacBook befestigen und ist mit einer Vielzahl von Geräten – wie Laptops, Smartphones, Tablets, Kameras und Spielekonsolen – kompatibel.

www.lexar.com

Hama

Für vollkommene Entspannung

© Hama GmbH & Co KG

Immer mehr Menschen setzen beim Einschlafen oder Yoga auf ruhige Musik oder Hörbücher. Der Hama Bluetooth-Kopfhörer „Spirit Calm“ hilft jetzt dabei. Er ist so klein und unscheinbar, dass er bei Bewegung weder verrutscht noch beim Liegen auf der Seite drückt. Die kabellosen Mini-Ohrhörer sind so bequem und leicht, dass sie auch nach längerem Tragen nicht stören – perfekt um voll und ganz abzuschalten. Die Laufzeit beträgt dabei vier Stunden bei vollgeladenen Earbuds und nochmal zehn Stunden nach 2,5-fachem Nachladen in der Ladeschale. Über den Akkustand der Ohrhörer informiert die LED-Anzeige am Ladecase. Des Weiteren hält der „Spirit Calm“ mit integriertem Mikrofon, einer Berührungssteuerung sowie den Sprachassistenten Siri und Google Assistant allen Anforderungen an einen modernen In-Ear-Kopfhörer stand.

www.hama.de

© Plaion

Plaion

8-BIT-NOSTALGIE IN VOLLENDUNG

Der legendäre Commodore 64 feiert ein stylishes Comeback: Die limitierte THEC64 mini – Black Edition kombiniert Retro-Charme mit moderner Technik. Schwarzes Design, neue Spiele und nostalgisches Feeling. Ein Must-have für Fans, Sammler und C64-Neulinge.

Der kultigste 8-Bit-Computer der Welt ist zurück und hat ein brandneues Makeover bekommen. Der THEC64 mini – Black Edition ist seit Oktober erhältlich und bietet eine handverlesene Bibliothek moderner C64-Meisterwerke sowie ein edles matt-glänzendes schwarzes Finish. Retro-Gaming in seiner stylishsten Form. Diese limitierte Neuauflage des Commodore 64 wurde von Retro Games Ltd. (RGL) in Zusammenarbeit mit Plaion Replai entwickelt und ist nicht nur ein Stück Nostalgie. Es ist eine lebendige Hommage an die Fans und Entwickler, die nie aufgehört haben, für die Hardware zu programmieren, die eine ganze Generation von kreativen Köpfen hervorgebracht hat. „Das ist kein Blick in die Vergangenheit, sondern eine Fortsetzung“, sagt Paul Andrews, Geschäftsführer bei RGL. „Die Black Edition zelebriert die Energie einer Community, die auch lange nach dem Ende der kommerziellen Ära weitergemacht, experimentiert und für Innovationen gesorgt hat. Sie ist der Beweis dafür, dass die Kreativität auf dem C64 nie erloschen ist.“

Von Hobby-Programmierern zu modernen Meistern. Als der Commodore 64 1982 auf den Markt kam, verwandelte er Millionen von Menschen in Entwickler. Jahrzehnte später treibt derselbe Geist noch immer eine weltweite Homebrew-Szene an, zu der eine lebendige DIY-Community gehört, die neue Spiele für alte Hardware entwickelt. Die THEC64 mini – Black Edition vereint diese Szene in einer definitiven Sammlung – 25 vorinstallierte, handverlesene Neo-Retro-Spiele, die von einigen der talentiertesten zeitgenössischen C64-Entwicklern erstellt wurden.

Back in black. Die Kampagne will die Underground-Ästhetik und die Kreativität der modernen C64-Szene würdigen. Mit ihrem schlanken schwarzen Design, Plug-and-Play-HDMI, vier Speicherplätzen pro Spiel und einem USB-Joystick mit Mikroschaltern ist diese Edition für Sammler, Programmierer und Neulinge gleichermaßen geeignet.

www.plaion.com

tastaturen.com

Für maritime Anwendungen

Mit der KWD-105S stellt tastaturen.com eine neu entwickelte Silkontastatur vor, die sich vor allem in den Bereichen Industrie, Militär und Marine bewährt. Das marinezertifizierte Gerät nach DIN IP68 hat eine steuerbare Hintergrundbeleuchtung, einen integrierten Trackball sowie eine Metallrückwand zum optimalen

© tastaturen.com

Schutz in rauen Umgebungen. Die Tastatur ist als Desktopgehäuse mit USB-Schnittstelle, auf Wunsch auch mit Befestigungsbolzen, lieferbar.

Große Leistung auf kleinstem Raum. Die Silikontastatur kommt mit den Abmessungen 309 x 127 x 16 mm auf den Arbeitsplatz. Der Tastenhub mit nur 1,5 mm gewährleistet eine angenehme Bedienung und eine gute taktile Rückmeldung. Die Tastatur ist mit 105 Tasten wie gewohnt im Standardlayout verfügbar, die Tastensymbole sind gelasert und abriebfest.
Insbesondere in maritimen oder militärischen Umgebungen ist eine vernünftige Beleuchtung unerlässlich. Bei der KWD-105S ist die Stärke der Hintergrundbeleuchtung über zwei Tasten justierbar. Die Stromversorgung liegt bei + 5 V/DC, 20 mA (Hintergrundbeleuchtung 400 mA).

www.tastaturen.com

© Concept International

Concept International

OFFICE-ALLROUNDER

Der FutureNUC Essential von Concept International ist ein Mini-PC mit großem Potenzial. Mit Intel-Quadcore, DDR5-Speicher und 8K-Support bietet er alles für moderne Office-Umgebungen – platzsparend und energieeffizient.

Mit dem FutureNUC Essential bietet der Münchner Value Added Distributor Concept International einen besonders günstigen Mini-PC seiner Hausmarke FutureNUC für den Einsatz in allen Büroumgebungen, die eine schnelle, kosteneffiziente und platzsparende Lösung für klassische Office-Aufgaben benötigen. Für Komfort und Effizienz bei der Arbeit bietet der kompakte Preis-Leistungs-Riese den Anschluss von zwei Monitoren mit 8K-Auflösung sowie schnelle 16 GB DDR5-Speichertechnologie in Verbindung mit einem aufrüstbaren, üppigen 256 GB SSD-Speicher.

Für gängige Office-Herausforderungen. Ob für die Erstellung von Dokumenten und Präsentationen, die Bearbeitung von Tabellen oder das Versenden von E-Mails – der Mini-PC FutureNUC Essential meistert jede gängige Office-Herausforderung. Aufgrund seines besonders kompakten Formfaktors mit rund 10 x 10 cm Fläche und nur 23 mm Höhe eignet sich der Mini-PC für den Einsatz auf kleinstem Raum und ist zudem ökonomisch im Stromverbrauch (durchschnittlich 10-12 Watt). Der kleine Office-Allrounder ideal für den Einsatz auch in großen Stückzahlen für Unternehmen jeder Größe geeignet, ob für moderne Office-Umgebungen wie New-Work-Bürokonzepte mit flexiblen Arbeitsplätzen, für Service- und Callcenter oder das Homeoffice.

Für alle Büroaufgaben. Der FutureNUC Essential ist mit Windows 11 Pro, Intel UHD-Grafik und einem Intel Quadcore N150-Prozessor mit 3,6 GHz ausgestattet, der die perfekte Leistung für Büroaufgaben und Office 365 bietet. Aktuellste Technik wie die superschnelle DDR5-Speichertechnologie (bis zu 64 GB), die bis zu 30 % schneller ist als DDR4-Vorgänger, sorgen für rasches Arbeiten. 250 GB bis 2 TB Storage bieten ausreichend Speicherplatz für Programme und Daten.

Flexible Anschlussmöglichkeiten. Für Komfort bei der Arbeit ermöglichen zwei HDMI 2.1-Ports (8K@60Hz) den Anschluss von Monitoren mit 8K-Auflösung. Flexibilität bieten insgesamt vier USB-Ports (2x USB 3.2 Gen 2, 2x USB 2.0). Intel Wi-Fi 6E und ein LAN-Port sorgt für beste Konnektivität. Über Bluetooth 5.3 können einfach und kabellos Peripheriegeräte wie Maus und Tastatur angeschlossen werden. Darüber hinaus gibt es einen High Definition Audio-Kopfhörer/Mikrofon-Anschluss.

www.concept.biz

© Samsung

Samsung

Start in neue digitale Welten

Mit Galaxy XR stellt Samsung sein neues AI-natives Gerät vor. Es ist das erste Produkt der neuen Android XR-Plattform, in die Gemini bereits auf Systemebene integriert ist. Damit fühlt sich das Gerät nicht wie ein Tool an, das Befehle ausführt, sondern wie ein AI-Begleiter, der Nutzer:innen hilft, ihre Aufgaben zu managen und sich natürlich und intuitiv per Sprache, Bild und Gesten steuern lässt. In Form eines Headsets versteht es die Umgebung der Nutzer:innen. Es sieht, was sie sehen, und hört, was sie hören. So kann Galaxy XR auf natürliche, gesprächsähnliche Weise reagieren und innovative Wege eröffnen, mit Technologie zu interagieren. Seit dem 21. Oktober ist das Headset in den USA und Korea erhältlich.

Komfortabel, leicht, robust. Galaxy XR wurde so entwickelt, dass Nutzer:innen es auch über längere Zeit komfortabel tragen können. Möglich machen dies ein spezielles Design, moderne Materialien und optimierte Bauteile. Durch die leichte und robuste Bauweise ist das Gerät alltagstauglich. Der ergonomisch ausbalancierte Rahmen verteilt den Druck angenehm auf Stirn und Hinterkopf und bietet sicheren Halt. Der Akku sitzt nicht direkt am Gerät, sodass es kompakt bleibt und bequem zu tragen ist. Samsung Galaxy XR verfügt zudem über einen abnehmbaren Lichtschutz. Er kann den Lichteinfall der Umgebung reduzieren, damit Nutzer:innen ungestört arbeiten, kreativ sein oder spielen können, egal ob sie gerade bei Google Maps, YouTube, Circle to Search mit Google oder Google Fotos unterwegs sind.

www.samsung.com

DAS EHZ-PARTNERPROGRAMM

Als Distributor bieten Sie Ihren Kunden interessante Produkte und einen professionellen Service. Die EHZ austria unterstützt Sie dabei. Als führende IKT-Plattform bringen wir internationale Hersteller, heimische Händler und nicht zuletzt Sie als wichtigste Drehscheibe an einen Tisch.

Denn Kommunikation ist alles.

allyouneed ONLINE GMBH

A-1220 WIEN • KONSTANZIAGASSE 31-35/2
TEL: (01) 285 87 78-0 • FAX: (01) 285 87 78-87

Produkte HP Inc., HP Enterprise, IBM, Dell, Lenovo, Fujitsu, Cisco, Netgear, D-Link, Zyxel, Epson, Canon, Lexmark, Kingston, APC, Samsung, Benq, AOC, Zebra, Moxa, Axis, TP-LINK, Logitech, Eizo, Qnap, Intel, AMD, Microsoft, Ubiquiti, Digitus
Ansprechpartner Michael Swoboda • Martin Pfeifer • Mag. Hertha Swoboda
Tel DW 99 • DW 33 • DW 88
E-Mail m.swoboda@ayno.at • m.pfeifer@ayno.at • h.swoboda@ayno.at
www.ayno.at

ALSO AUSTRIA GMBH

A-2301 GROSS-ENZERSDORF • INDUSTRIESTRASSE 14
TEL: (02249) 7003-0 • FAX: (02249) 7003-119

ALSO Austria GmbH ist ein führender Technologieanbieter und Teil der ALSO Holding AG. Das Unternehmen bietet Lösungen in ITK-Infrastruktur, Cloud, Cybersecurity, IoT und Digitalisierung. Themen wie Kreislaufwirtschaft, Finanzierungsmodelle, Mietlösungen mit Rückkauf und Mitlizensierung sind zentral. Partner profitieren von IoT-Plattformen, Hardware, sowie Value Added Services wie Pre-Sales Support für Cloud-, Rechenzentrum- und Hybridlösungen. Das starke ALSO-Ökosystem steigert Effizienz und Umsatz, mit Fokus auf Nachhaltigkeit und digitale Transformation.
Produkte Hardware, Software, PCs, Notebooks, Tablets, PC-Komponenten, Server, Storage, Netzwerkkomponenten, Telekommunikation, Supplies, Drucker, BTO, e-Service & Dienstleistungen, Cloud-Services
Hersteller > 200
Ansprechpartner Martin Poglin, Geschäftsführer
E-Mail martin.poglin@also.com
www.also.at
www.alsocloud.at

AMEA GROSSHANDELSGMBH

A-1130 WIEN • WINKELBREITEN 37/1
TEL: (01) 512 81 81 • FAX: (01) 512 81 81-25

Hersteller: Aten, Dätwyler, Eaton, Neol, Datalocker, Roline, Value, Bachmann, Vivotek
Produkte: Aten (KVM und Fernwartung), Dätwyler (Europäische Netzwerkkabel), Eaton (USV und Stromversorgung), Neol (IP Stromverteiler und Remote Monitoring), Datalocker (Verschlüsselungslösungen), Roline/Value (IT-Zubehör und Netzwerktechnik), RolineGREEN (Umweltschonende Verpackung: Papieretikett, TPE- oder LSOH-Material, keine Plastiktüten und Kunststoffkabelbinder), Sonderkonfigurationen für Kabel
Ansprechpartner: Gerhard Feichter • Michael Schwiesow
Tel DW: 10 • DW 11
E-Mail: verkauf@amea.at
www.amea.at

API ÖSTERREICH GMBH

A-2700 WIENER NEUSTADT • WIENERSTRASSE 111-115 / 1.2.F.
TEL: +43 (0) 50 21 55 -0

Hersteller: mehr als 400 Hersteller im Portfolio; rund 130.000 Artikel
Warengruppen / Produktbereiche: Mobile Computing/Components/PC-Systeme/Server/Gaming/Peripherie/Bildschirme/Signage/Drucker/Netzwerk/Verbrauchsmaterial/Education/Medical/Software/Bürobedarf-einrichtung/Haushalt
Lösungen: ESD/Fulfillment/Office Solutions/Project Support
Dienstleistungen: BTO/Laser-Customizing/Api-Cloud/EDI-Support (Cop/iT-Scope/uvm.)
Ansprechpartner: Christian Gretschi (GF); Michael Anzeletti (TL); Henrik Rateniek (TL)
E-Mail: vertrieb@api-oesterreich.at
www.api-oesterreich.at

AQIPA GMBH

A-6250 KUNDL • MÖSLBICHL 78
TEL: +43 (0)5332 72300 • FAX: +43 (0)5332 72300-300

Produkte Computer, App & Apple/Android Zubehör / Kopfhörer / Fototaschen, Beats by Dr. Dre, Case Logic, Golla, Kensington, Libratone, Monster Audio, Monster Cable, Runtastic, SOL Republic, TDK, Thule, WeSC, XtremeMac
Ansprechpartner Klaus Trapl
E-Mail info@aqipa.com
www.aqipa.com

ARROW ECS GMBH

A-4040 LINZ • FREISTÄDTERSTRASSE 236
TEL: (0732) 75 71 68-254 • FAX: (0732) 75 71 44

Produkte Value-Added Distributor für Security, Storage, Server-Infrastruktur und Software (z.B. Check Point, Kaspersky Lab, NetApp, VMware, Symantec, Oracle, RSA)
Ansprechpartner Ines Bandzauner, Marketing Manager
Tel (0732) 75 71 68 • DW 254
E-Mail ines.bandzauner@arrow.com
www.arrow.com/globalecs/at/

ASTCO GMBH

A-1020 WIEN • HANDELSKAI 265
TEL: (01) 72 751-0 • FAX: (01) 72 751-33

Produkte Storage-Lösungen: Raid, San, Nas, Storage-Virtualisierung, Backup
Ansprechpartner Erwin Zawadil
Tel DW 17
E-Mail verkauf@astco.com
www.astco.com

BOLL AUSTRIA GMBH

A-1100 WIEN, WIENERBERGSTRASSE 3-5
TEL.: +43 (1) 235 00 65 • E-MAIL: AUSTRIA@BOLL.CH

BOLL ist der führende Trusted Advisor Distributor für IT-Security- und Networking-Produkte in der Schweiz und hat sich im Laufe der Jahre vom lokalen IT-Security-VAD zum umfassenden Cybersecurity-Spezialisten in DACH entwickelt.
Das eigentümergeführte Unternehmen wurde 1988 gegründet und steht für ein Höchstmass an Engagement, Erfahrung und Kompetenz sowie für Expertenwissen und Services.
Hersteller: Alcatel-Lucent Enterprise, Asimily, Claroty, Cyolo, DeepInstinct, Fudo, Kaspersky, Menlo Security, Netskope, OneSpan, Palo Alto Networks, Proofpoint, SEPPmail / Swiss Sign, Varonis, Wallix
Ansprechpartner Irene Marx, Geschäftsführerin
www.boll.ch

CANON AUSTRIA GMBH

AM EUROPAPLATZ 2 • 1120 WIEN
TEL.: +43 (1) 68088-0 • FAX +43 (1) 68088-788

Produkte In einer sich schnell verändernden digitalen Welt stehen wir Ihnen mit neuen Möglichkeiten und Innovationen zur Seite, die von einem radikal neuen Denken geprägt sind. So verbessern wir die Art und Weise, wie Menschen zusammen arbeiten und leben. Entdecken Sie unser umfangreiches Business Produkt-Portfolio und optimieren Sie Wachstum und Produktivität mit unseren innovativen Lösungen.
Bürodrucker, Fax und multifunktionale Systeme, Großformat-Drucksysteme, Produktions- und kommerzielle Drucker, Business Software/IT Services, Scanner, Medical Systems, Projektoren, Netzwerkkameras, Tinte Toner&Papier
E-Mail info@canon.at, direktvertrieb@canon.at
www.canon.at

BARCOTEC GMBH

A-5020 SALZBURG, JULIUS-WELSER-STRASSE 15
TEL: 0662 424 600 • FAX: 0662 424 601
A-1150 WIEN, MÄRZSTRASSE 1
TEL.: (01) 786 39 40 • FAX: (01) 786 39 41

Hersteller Direktimporteur und Distributor für DENSO Wave, Datalogic, industrielle Datenbrillen von RealWear, Citizen, Honeywell, Zebra, Feig und M3 Mobile
Produkte Mobile Computer, Industrielle Datenbrillen, Wearables, Rugged Tablets, Fahrzeugterminals, Handscanner, RF-ID Equipment, Barcode- und RFID-Drucker
Ansprechpartner Alexander Humer, Msc
E-Mail sales@barcotec.at
www.barcotec.at

BROTHER INTERNATIONAL GMBH, ZWEIGNIEDERLASSUNG ÖSTERREICH

A-1120 WIEN, AM EUROPLATZ 2, STIEGE 2, 3.OG-M1
TEL.: +43 (1) 610 13-0 • FAX: +43 (1) 610 13-4300

Produkte Farb- und Monochrom-Drucker, Multifunktionsgeräte (Drucken, Kopieren, Scannen, Faxen), Dokumenten-Scanner, Etikettendrucker, Beschriftungssysteme (P-touch)
Tel Vertriebsinnendienst DW 4350
E-Mail auftragsbearbeitung@brother.at
www.brother.at

EXCLUSIVE NETWORKS AUSTRIA GMBH

A-2345 BRUNN AM GEBIRGE / HEINRICH BABLIK-STRASSE 17, K21, TOP N06
INFO.AT@EXCLUSIVE-NETWORKS.COM / TEL: +43 (1) 336 0 337-0

Exclusive Networks ist als Value Added Distributor (VAD) Ihr globaler Cybersecurity-Spezialist, der Partnern und Endkunden eine einzigartige Kombination von Dienstleistungen und Produktportfolio bietet.
Hersteller: Arista, Axonius, BeyondTrust, Cubbit, Exabeam, ExtraHop, Extreme Networks, Forescout, Fortinet, Imperva, Infoblox, iQSol, LogRhythm, Netskope, Nozomi Networks, Okta, One Identity, Opengear, Palo Alto Networks, Proofpoint, Rackmount IT, Rubrik, Salt Security, SentinelOne, Tanium, Thales, ThriveDX, Wasabi
Value Add: Trainingscenter für Fortinet, Infoblox, Palo Alto Networks & SentinelOne. Unser Pre-Sales Team unterstützt Sie bereits zu Beginn von Projekten mit Beratung und der Ausarbeitung möglicher Lösungen. Als autorisierter Supportpartner vieler unserer Hersteller bieten wir Ihnen gerne Supportleistungen an, die das Angebot einzelner Hersteller erweitern.
E-Mail vertrieb.at@exclusive-networks.com
www.exclusive-networks.com/at

HEADON COMMUNICATIONS GMBH

A-1030 WIEN, MARXERGASSE 25
TEL.: (01) 7431493 372, FAX (01) 7431493 122

Produkte Headsetlösungen von Jabra, VoIP-Anlagen von 3CX; IP-DECT und Alarmierungssysteme von ASCOM und RTX; ISDN-Gateways von Beronet; VoIP-Telefone von Snom, Yealink
Ansprechpartner Marina Auer • Rene Horvath
Tel (01) 7431493 372
E-Mail reseller@headon.at
www.headon.at

INFINIGATE ÖSTERREICH GMBH

A-1220 WIEN • HIRSCHSTETTNER STRASSE 19
TEL: (01) 890 21 97-0 • FAX: (01) 890 21 97-157

Produkte A 10 Networks, Armis, Barracuda, Belden, Bitdefender, BlackBerry, Cato Networks, Check Point, Cloudflare, conpal by Utimaco, Cybereason, Datto, Entrust, Extreme Networks, Forcepoint, Fortra, HID, Hornetsecurity, HPE aruba Networking, Kaspersky, Lywand, Microsoft, Netscout, Progress, Rapid7, Riverbed, Ruckus Commscope, Sekoia, SentinelOne, SEPPmail, Skyhigh Security, SonicWall, Trellix, TXOne, Vectra, Versa Networks, WatchGuard, Yubico
Ansprechpartner Florian Jira
Tel DW 100 Vertrieb • DW 200 Logistik
E-Mail florian.jira@infinigate.at
vertrieb@infinigate.at
www.infinigate.at

INGRAM MICRO GMBH

A-1020 WIEN • JAKOV-LIND-STRASSE 5/1. OG
TEL: +43 1 408 15 43-0

Produkte In den Bereichen PC, Server/Storage, Displays, Tablets, Software, Mobiles, Peripherie, Komponenten, Drucker & Supplies, Netzwerk, Cloud, Digital Signage, Security, Unified Communications, Data Capture/Point of Sale (DC/POS)
Hersteller > 200 über alle Produktbereiche
Kontakt +43 1 408 15 43-0
E-Mail office.at@ingrammicro.com
at.ingrammicro.com

M.K. COMPUTER ELECTRONIC GMBH

A-1230 WIEN • RICHARD-STRAUSS-STRASSE 12
TEL: (01) 616 30 30 • FAX: (01) 616 30 30-30

Produkte Distribution aller Ersatzteile von HP/Compaq, Kyocera, Lexmark, IBM/Lenovo, Ricoh, Canon, Acer, Fujitsu, Xerox, Brother, Samsung, Oki, Asus, Dell, Toshiba, Zebra
Ansprechpartner Alexander Rein
E-Mail vertrieb@mk-electronic.at
www.mk-electronic.at

NESTEC SCHARF IT-SOLUTIONS OG

A-4490 ST. FLORIAN • PUMMERINPLATZ 5
TEL: (07223) 80703-0

Produktbereiche Netzwerk-, Mail- & Online Security, Netzwerk-Management, Cloud Solutions, Lösungen für MSP's (RMM, MSP Management, Security as a Service)
Hersteller/Marken Altaro * Anydesk * Dogado * ESET * GFI Software * Hornetsecurity * ManageEngine * Parallels * Pulseway * Vipre * Wasabi * XCAPI * ZOHO sowie AATL, SSL & S/Mime Zertifikate und die Eigenprodukte MSP Business Manager, MSP MailProtection, MSP RMM und AgreeGate
Partnerschaft mit Barracuda und Lancom
Ansprechpersonen Alexander Scharf – GF Software & Services
Harald Scharf – GF Hardware & Consulting
E-Mail vertrieb@nestec.at • office@nestec.at
https://nestec.at

OMEGA HANDELSGESELLSCHAFT M.B.H.

A-1230 WIEN • ERNST-KRENEK-GASSE 4
TEL: (01) 615 49 00-0

Produkte Acer, Adlink, AMD, AOC, ASRock, Apple, Canon, Chief, Corsair, Crucial, Cybernet, Dell Technologies, Digitus, Eaton, Eizo, Elgato, Ergotron, Evoko, HP, HPE (Hewlett Packard Enterprise), iiyama, Intel, Kyocera, Lenovo, LG, Lindy, Logitech, Man&Machine, Maxdata, Microsoft, MSI, Peerless, Philips, Proworx, Renewd, Samsung, Seagate, Sharp/NEC, Shuttle, SMS, Thrustmaster, Trisa, Western Digital
Geschäftsführung Florian Wallner & Martin Eckbauer
E-Mail verkauf@omegacom.at
www.omegacom.at

SHARP ELECTRONICS (EUROPE) GMBH

ZWEIGNIEDERLASSUNG ÖSTERREICH • A-1020 WIEN • HANDELSKAI 342
TEL.: (01) 727 19-0 • FAX: (01) 727 19-285

Produkte: Visual Solutions, Displays, Interaktive Whiteboards, Kassen/POS-Systeme
Ansprechpartner: Harald Wagner (Visual Solutions), Christoph Wagner (Indirect Sales)
Tel Harald Wagner DW 215 • Christoph Wagner DW 210
E-Mail harald.wagner@sharp.eu, christoph.wagner@sharp.eu
www.sharp.at

SYSTEAM GMBH

A-1230 WIEN • OBERLAAER STRASSE 331
TEL: (01) 6152549-0 • FAX: (01) 6152549-16

Produkte Drucker, Verbrauchsmaterial, Druckerzubehör, Peripherie, Hardware, Software, Notebooks, Monitore, Desktops, Server, PC-Komponenten, Netzwerkkomponenten, Scanner, 3D-Drucker
Hersteller 3M, Acer, Apple, Asus, Brother, Canon, DELL, Dicota, Epson, Fujitsu, HP, Iiyama, Intel, LG, Konica Minolta, Lenovo, Logitech, Kyocera, Lexmark, Microsoft, Oki, Panasonic, Plustek, Ricoh, Samsung, SEH, Silex, Xerox
Ansprechpartner Eduard Pacher, Michael Pregesbauer, Thomas Ungar, Robert Dragotinits
Tel (01) 6152549-0
E-Mail office@systeam-austria.at
www.systeam-austria.at

QUORUM DISTRIBUTION GMBH

AM EUROPLATZ 2 • GEBÄUDE 4
1120 WIEN

Hersteller Arctera, Arista, Cirrus Data, Cohesity, Cofense, Fast LTA, Keepit, Komprise, NetApp, Nasuni, Quantum, ProLion, Pure Storage, RNT Rausch, Rubrik, Symon
Value Add Ready | Easy | Local | Reliable | Focused
Quorum ist Spezialist für Datenverfügbarkeit und kombiniert technisches Know-how mit Engagement und Kundennähe. Wir realisieren maßgeschneiderte Backup- und Storage-Lösungen mit hochwertigen Produkten ausgewählter Hersteller – unabhängig von Projektgröße. Dabei sind wir schnell einsatzbereit (Ready), einfach in der Zusammenarbeit (Easy), lokal verankert (Local), zuverlässig (Reliable) und stets fokussiert auf individuelle Anforderungen (Focused).
Geschäftsführung Alexander Paral (apa@quorum.at)
Tel +43 1 36 119 66-0
E-Mail info@quorum.at
www.quorum.at

TD SYNNEX AUSTRIA GMBH

A-1120 WIEN • KRANICHBERGGASSE 6 / EUROPLAZA K
TEL: (01) 61488-0 • FAX: (01) 61488-80

Hersteller mehr als 200 Hersteller, darunter: Adobe, APC, Apple, Autodesk, Cisco, Dell Technologies, Epson, Hewlett Packard Enterprise, HP, Hitachi, IBM, iiyama, Intel, Lenovo, Lexmark, Logitech, Microsoft, Oracle, Oculus, Samsung, Synology, VEEAM, VMware, Western Digital, Xerox

Produkte Components, Server, Storage, Networking, Software, Cloud, Tablets, Mobile, PC´s, Notebooks, Peripherie, Printer, Supplies, Displays, Conferencing, Collaboration, Digital Signage, POS-Systeme, Consumer Electronic, Gaming, Smart Home

Lösungen Cloud Computing-, Open Shift- , Converged Infrastructure-, Datacenter- Solutions, Virtualisierung, Security, Iot & Analytics, Gaming, Smart Home, Conferencing & Collaboration, Mobility, Office Solutions, Infrastructure-HW, Unified Communication

Dienstleistungen/Services e-services und Dienstleistungen, Cloud Services, Trainings, Zertifizierungen, Implementations & Beratungs- Services, WaaS, DaaS & TaaS, Logistik-Services, Finanz-Services, Leasing, BTO-Services

Ansprechpartner Michael Sewald, Alexander Kremer, Daniel Zenz

E-Mail sales.at@tdsynnex.com

www.at.tdsynnex.com/blog
www.at.tdsynnex.com

TARGET DISTRIBUTION GMBH

A-6842 KOBLACH • STRASSENHÄUSER 59
TEL: +43 5523 54 871-0

Hersteller Apple, JBL, Beats, Eve, LaCie, OWC, Satechi, Trunk, Zagg, Mophie, Lexon, XP Pen, TP Vision, Dbramante, Brother, PARAT, Withings, Backbone, Iiyama.
Leistungen Als Österreichs führender Value Added Distributor in der IT-Branche stehen wir für hochwertige Produkte, kompetente Beratung, einen exzellenten Service, innovative Lösungen sowie über 45 Jahre Erfahrung.
Services/Tools Apple autorisierter Service Provider mit speziellem Reparatur-Tool, Apple Distribution Partner Programm, spezielle Apple Tools wie CTO Konfigurator, Apple Care+, DEP & VPP, Altgeräteankauf. E-Commerce-Tools: Target Webshop, B2C-Shop Anbindungen, Gustav Preislistenmodul sowie diverse Anbindungen wie z.B.: EDI.
Ansprechpartner Martin Poglin, Roman Thiel
E-Mail info@target-distribution.com
www.target-distribution.com

TFK HANDELS GMBH

A-5302 HENNDORF • LANDESSTRASSE 1
TEL.:+43 6214 6895 • FAX +43 6214 6872

Hersteller Alle namhaften Hersteller (u.a. A1, Apple, Agfeo, Alan, Alcatel, Emporia, Gigaset, Huawei, Metz, Mitel, Nokia, Panasonic, Samsung, Sony, Sharp oder Xiaomi) sowie Newcomer mit innovativen Nischenprodukten.
Produkte Maßgeschneiderte Distribution, Logistik (von b2b bis b2c), Schulungen, Betreuung und (online SIS) Shop-Lösungen.
Bereiche (Vollsortiment) Telekommunikation, A1 Anmeldeservice, Festnetztelefonie (SOHO bis BIG), Funk, Smart Home, Haussteuerung, Kommunikationssysteme, Überwachungskamera (Reviermanager), Zubehör und Consumer Electronic. Datenübertragung und Analyse Software, Voice over IP, Netzwerklösungen sowie (CE) TV over IP.
Ansprechpartner Roswitha Lugstein, Alexander Meisriemel, Stefan Windhager
E-Mail partner@tfk-austria.at
www.tfk-shop.at
www.reviermanager.at
www.tfk-austria.at

TOTAL-INFORMATION-MANAGEMENT TIM AG

A-2351 WIENER NEUDORF • IKANO BÜROHAUS 2, 1.ST. TOP 158, TRIESTER STRASSE 14
TEL: +43 (2236) 20 57 00-20 • FAX: +43 (2236) 20 57 00-99

Hersteller: DELL Technologies, Lenovo, Nutanix, PureStorage, Barracuda, Quantum, BitDefender, ArcServe, Veritas, Virtual Solution, Overland-Tandberg, Cohesity, ProLion, ...
Produkte: Value-Added Distribution für DataCenter Infrastructure, Cloud-, Netzwerk- und Security-Lösungen
Leistungsportfolio: Business Development, Enablement, Ausbildung und Zertifizierungssupport, Projektunterstützung, PreSales, Consulting, Implementierung, Professional IT-Services, ...
Ansprechpartner: Vorstand Christian Moser (ChristianM@TIM-VAD.at)
Vertrieb: E-Mail: Vertrieb@TIM-VAD.at; Tel.: +43 (2236) 20 57 00 DW: 310
www.TIM-VAD.at

UFP AUSTRIA GMBH

A-5310 MONDSEE • WALTER-SIMMER-STRASSE 9
TEL.: (06232) 33 99-0 • FAX: (06232) 26 92-0

Produkte Distributor für Produkte namhafter Hersteller in Top Qualität:
Drucker und Druckerverbrauchsmaterial von HP, Brother, Canon, ... sowie Computer-, Telekom- und Bürozubehör
Vertrieb von PV-Anlagen und Solarenergieprodukten.
Hohe Verfügbarkeit vom Alltagsartikel bis hin zum High-End Produkt.
Ansprechpartner Patrick Rindberger
Tel DW 63
E-Mail p.rindberger@ufp.at
www.ufp.at

WESTCON GROUP AUSTRIA GMBH

A-2355 WR. NEUDORF • IZ-NÖ-SÜD • STRASSE 7 OBJ. 58C
TEL: +43 2236 8644 44 0

Produkte Westcon-Comstor ist ein Value Added Distributor führender Security-, Collaboration, Netzwerk- und Datacenter-Technologien und hat mit innovativen, weltweit verfügbaren Cloud-, Global Deployment- und Professional Services die Lieferketten in der IT neu definiert. Das Team von Westcon-Comstor ist in über 70 Ländern präsent und unterstützt seine Partner mit maßgeschneiderten Programmen und herausragendem Support dabei, ihr Business kontinuierlich auszubauen. Langfristig ausgelegte, stabile Geschäftsbeziehungen ermöglichen es, jeden Partner individuell und bedarfsgerecht zu betreuen.
E-Mail sales.at@westcon.com, sales@comstor.at
www.westcon.com
www.comstor.at

EHZ austria
INDEX-HOTLINE
+43 (0) 664 200 50 09

Der EHZ Distributoren- und Hersteller-Index

Ein ganzes Jahr lang präsent – ab 300 Euro

Ihr Unternehmen agiert als Drehscheibe zwischen Herstellern und dem Fachhandel? Sie bieten dem Handel ein interessantes IKT- und UE-Produktsortiment? Im völlig neu konzipierten Distributoren– und Hersteller-Index haben Sie die Gelegenheit, gegen einen geringen Unkostenbeitrag in jeder Ausgabe der EHZ austria mit Ihren wichtigsten Unternehmensinformationen vertreten zu sein.

Top-präsent
mit Ihrem
Logo-Eintrag
um nur
€ 300,- pro Jahr

Aufbau des Logo-Eintrags:
- Firmenname, Adresse
- Telefon- und Faxnummer
- Produkte/Produktgruppen (max. 6)
- Ansprechpartner (max. 5)
- Tel.: der Ansprechpartner
- E-Mail-Adressen der Ansprechpartner
- **Ihr Logo in 4c**

MUSTERMANN GMBH
A-1020 WIEN • DABINICHGASSE 265
TEL: (01) 21 22 23-0 • FAX: (01) 21 22 23-33
Produkte Storage-Lösungen: Raid, San, Nas, Storage-Virtualisierung, Backup
Ansprechpartner Oskar Partner
Tel: DW 17
E-Mail verkauf@mustermann.com
www.mustermann.com

AS media
Mag. Andreas Slama

NEU

Verknüpfen Sie Ihren Top-Logo-Eintrag mit unserem neuen Online-Index. Wir übernehmen Ihre Daten und verlinken ihn mit Ihrem Online-Auftritt. So werden Sie noch besser gefunden. + € 150,-

Ja, ich bestelle

☐ **Top Logo-Eintrag für ein Jahr um € 300,-**

☐ **Zusätzlicher Eintrag im Online-Index € 150,-** (nur in Kombination mit einem Print-Eintrag buchbar)

Preise in Euro zzgl. 5 % Werbeabgabe und exkl. 20 % MwSt., der Betrag ist sofort nach Rechnungserhalt zahlbar, gilt für 12 Monate und wird jeweils im zwölften Monat für das Folgejahr verrechnet. Der Auftrag gilt bis auf Widerruf als unbefristet abgeschlossen.
Im Preis inkludiert ist ein Jahresabo von EHZ austria.

Firmenname

PLZ / Ort | Adresse

Tel. | Fax:

Produkte

Ansprechpartner

Tel.-DW

E-Mail

www

Datum | Unterschrift

Nützen auch Sie den Distributoren- und Hersteller-Index für Ihre dauerhafte Präsenz beim Fachhandel!

Füllen Sie den obenstehenden Kupon bitte deutlich lesbar aus und senden Sie ihn per Post an die Verlagsadresse oder senden Sie die erforderlichen Daten per Mail an andreas.slama@ehzaustria.at.
Ihr druckfähiges Logo senden Sie bitte ebenfalls an andreas.slama@ehzaustria.at.

VORSCHAU
EHZ 09 2025

Die nächste Ausgabe erscheint am 12. Dezember 2025 mit folgenden Top-Themen:

BRANCHE
Trends, Marktpotenziale, Neuheiten ...

... Kooperationen, Übernahmen und Zusammenschlüsse, kurz: das Wichtigste aus der Welt des IT-Business – kompakt und übersichtlich zusammengefasst.

CHANNEL
Die Welt der Hersteller und Partnerprogramme

Hier lesen Sie alles Wissenswerte über die Partnerprogramme der Hersteller und Anbieter und erfahren die Strategien und Ziele der Channel-Verantwortlichen. Unser Fokus-Thema: Marketplaces. Diese wachsen rasant und verändern den Vertrieb. Wir werfen einen Blick auf Trends, Chancen und Herausforderungen.

TECHNIK
Smart Home – Intelligentes Wohnen

© rawpixel.com/Freepik

Vernetzte Geräte, digitale Assistenten und automatisierte Abläufe machen das Zuhause komfortabler und sicherer. Doch wie smart ist das smarte Wohnen wirklich – und wo liegen die Chancen und Grenzen der Technologie?

Notebooks – Mobil arbeiten

Leicht, leistungsstark und flexibel: Notebooks bleiben das Herzstück moderner Arbeitswelten. Wir zeigen, wohin sich der Markt bewegt, welche Trends die Hersteller setzen – und worauf Unternehmen beim Kauf jetzt achten sollten.

© benzoix/Freepik

Bestellen Sie jetzt Ihr EHZ-Abo!

Abonnieren Sie die EHZaustria und bekommen die neuesten Informationen aus Branche und Handel jedes Monat bequem nach Hause!
Schicken Sie Ihre Anmeldung per Mail (**andreas.slama@ehzaustria.at**) oder bestellen Sie unter **www.ehzaustria.at**! Einfacher geht's nicht! Ein Jahresabo kostet Sie nur 30 Euro!

EHZ austria

Impressum

Medieninhaber und Verleger
AS media, Mag. Andreas Slama
Lautensackgasse 29/11, 1140 Wien
Tel.: +43 (0) 664 200 50 09
Mail: andreas.slama@ehzaustria.at
www.ehzaustria.at

Geschäftsführung
Mag. Andreas Slama

Chefredaktion
Mag. Barbara Sawka
Mail: barbara.sawka@ehzaustria.at

Redaktionelle Mitarbeit
Mag. Susanna Thie

Anzeigenverkauf/-marketing
Mag. Andreas Slama
Tel.: +43 (0) 664 200 50 09
Mail: andreas.slama@ehzaustria.at

Art Direction
Tom Sebesta

Alle angegebenen Preise sind ohne Gewähr und inkl. MwSt. Der Verlag nimmt Manuskripte zur kostenlosen Veröffentlichung an. Honorare ausschließlich nach Vereinbarung. Für unverlangt eingesandte Manuskripte wird keine Verantwortung übernommen. Nachdruck oder Kopien von Beiträgen bzw. Teilen davon nur mit Genehmigung. Der Verlag behält sich vor, Beiträge auch in anderen verlagseigenen Zeitschriften zu publizieren bzw. für Sonderdrucke zu verwenden.

Einzelheft € 4,30
Jahresabonnement € 30,–
Grundlegende Ausrichtung der EHZaustria:
Ein unabhängiges Fachmagazin, das Reseller in den Bereichen IT und Telekommunikation über relevante und betriebswirtschaftliche Neuerungen informiert.

AS media
Mag. Andreas Slama

HAUS DER BARMHERZIGKEIT 150

Kleine Spende. Großes Lächeln.

Bewohnerin Maria, 102 Jahre alt, mit Pfleger Stefan

Jetzt kranken Menschen *Lebensfreude schenken!*

Seit 150 Jahren steht das Haus der Barmherzigkeit mit Einrichtungen in Wien und Niederösterreich für **professionelle und liebevolle Langzeitpflege und -betreuung. Mit Herz und Kompetenz** sowie modernsten Pflege- und Betreuungsansätzen, **ermöglichen wir chronisch kranken Menschen mehr Lebensqualität. Mit Ihrer Hilfe!** Denn nicht alle Leistungen werden von öffentlicher Hand finanziert. Damit wir die nötigen **Therapien und Lebensqualität** unserer schwer kranken Bewohner*innen **sicherstellen** können, brauchen wir Ihre Unterstützung. **Herzlichen Dank für Ihre Spende!**

Unser Spendenkonto:
Institut Haus der Barmherzigkeit
Raiffeisenlandesbank NÖ-Wien
IBAN: AT75 3200 0000 0044 4448
www.hb.at/jetzt-spenden

ÖSTERREICHISCHES SPENDEN GÜTESIEGEL 05304 WWW.OSGS.AT

Institut Haus der Barmherzigkeit | Seeböckgasse 30a, 1160 Wien | T +43 1 401 99-0 | info@hb.at | www.hb.at