VON IDG

COMPUTERWOCHE

Ausgabe 2021 – 29-30 19. Juli 2021 Nur im Abonnement erhältlich

VOICE OF DIGITAL

Cyber-Notstand in Anhalt-Bitterfeld

Hacker legen Verwaltung mit Ransomware lahm und fordern Lösegeld.

Seite 10

BMW optimiert seine Supply Chain

Um Engpässe zu vermeiden braucht es mehr Transparenz in der Lieferkette.

Seite 36

Personaler denken nicht digital

Die HR-Abteilung hinkt bei der Digitalisierung anderen Fachbereichen hinterher.

Seite 40

Tools gegen Hackerangriffe

Ransomware richtet Millionenschäden an. Werkzeuge wie Multi-Factor-Authentifizierung können davor schützen.

Seite 12

Es geht voran in Digital Germany

Auch wenn Hackerbanden Betriebe und Behörden terrorisieren: Die Digitalisierungserfolge hierzulande sind unübersehbar, wie der Wettbewerb Digital Leader Award 2021 zeigt.

Heinrich Vaske, Editorial Director

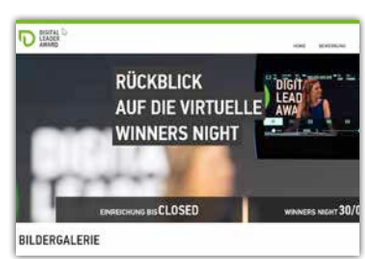
Ist doch klar, ruft mir die Kollegin durch ihren Mundschutz zu, in dieser Woche musst du die Kolumne über Cyberkriminalität schreiben. Unglaublich, was da gerade abgeht: die Ransomware-Attacken auf JBS Food und Kaseya (siehe Seite 12), hierzulande der Angriff auf das Landratsamt Anhalt-Bitterfeld und dann der neue Kalte (Cyber-)Krieg zwischen den USA und Russland.

Doch sich damit herumzuschlagen, ist einfach nur deprimierend. Sollen sich die Tageszeitungen darum kümmern, das Thema ist ohnehin ein politisches. Perfekt ausgestattete und organisierte Cybergangster-Banden arbeiten – staatlich sanktioniert oder zumindest unbehelligt von ihren Regierungen – daran, Unternehmen und ganze Volkswirtschaften zu beschädigen. Ein weltweit koordiniertes Vorgehen dagegen wird es nicht geben, genauso wenig wie gegen andere globale Bedrohungen wie den Klimawandel oder die Coronapandemie.

Bevor wir hier aber depressiv oder zynisch werden, wollen wir uns lieber einem erfreulichen Thema zuwenden – dem Digitalisierungsfortschritt in Deutschland. Mit der Verleihung der Digital Leader Awards (DLA) 2021 konnten COMPUTERWOCHE und CIO-Magazin einmal mehr zeigen, dass es hier allen Unkenrufen zum Trotz in großen Schritten vorangeht. Künstliche Intelligenz, Smart Factory, Mixed Reality, sogar Blockchain – viele dieser Technologen sind in der hiesigen Wirtschaft angekommen und sorgen in den Betrieben für teils spektakuläre Erfolge (siehe Seite 32). Trotz gegenläufiger Signale aus Bereichen wie Homeschooling, E-Government und Breitbandausbau geht es voran in Digital Germany. Bleibt zu hoffen, dass es so bleibt. Wichtigste Voraussetzung: Die Betriebe müssten ihre Hausaufgaben in Sachen Cybersicherheit machen ...

Herzlich,
Ihr

Heinrich Vaske, Editorial Director



Die Preisträger beim DLA:

Alles über Deutschlands führenden Digitalisierungswettbewerb Digital Leader Award 2021 finden Sie unter: digital-leader-award.de

Titelfoto: Anson/Shutterstock

12

Wie sich Unternehmen gegen Datenklau und Hackerbanden wehren können

Die Sicherheitslage im Cyberraum verschärft sich. Geheimdienste spähen Daten aus, und Hackerbanden legen mit Ransomware immer mehr Firmen und öffentliche Verwaltungen lahm. Wie der Kaseya-Hack gezeigt hat, können Betriebe im Grunde niemandem mehr trauen. Umso wichtiger werden eigene Security-Maßnahmen. Doch Tools wie Multi-Factor-Authentifizierung (MFA) wollen sorgfältig implementiert sein. Sonst hilft auch das beste Sicherheits-Werkzeug nicht weiter.

Markt

6 Landwirtschaft 4.0
Der Agrarsektor muss sich tiefgreifend verändern, hat eine Expertenkommission festgestellt. Digitale Tools können der Schlüssel für mehr Nachhaltigkeit und Umweltschutz sein, ohne Produktionseinbußen hinnehmen zu müssen.

8 Microsoft kauft RiskIQ
Mit Hilfe von Cyber Threat Intelligence sollen Microsoft-Kunden künftig ihre zunehmend heterogener zusammengesetzten Infrastrukturen besser absichern können.

11 Startups geben Politik schlechte Note
Startups beklagen schlechtere Rahmenbedingungen in Deutschland. Den Gründerinnen und Gründern fehlt es vor allem an der Unterstützung durch die Politik.

Technik

20 Die Storage-Zukunft ist die Cloud
Für viele CIOs wird Enterprise Storage zu einer strategischen Frage. Denn die Herausforderungen wachsen: steigende Datenmengen, die Gefahr von Cyberangriffen sowie der Trend zu hybriden Cloud-Modellen.

24 Cloud Security im Vergleich
Lesen Sie, welche Sicherheits-Features die großen Cloud-Anbieter AWS, Google und Microsoft zu bieten haben und auf was Anwender in Sachen Cloud Security besonders achten sollten.

28 HPE übernimmt Zerto
Mit den Zerto-Tools für Continuous Backup und Desaster Recovery will HPE seinen Kunden einen besseren Schutz gegen Attacken mit Erpressersoftware bieten.

Praxis

32 **Digital Leader Award 2021**
COMPUTERWOCHE und CIO-Magazin haben die spannendsten Digitalprojekte Deutschlands ausgezeichnet. Die vielen Initiativen und Leuchtturmprojekte machen deutlich, in welchen tiefgreifenden Transformationsprozessen viele Unternehmen stecken.

36 **Wie BMW die Supply Chain optimiert**
Für den Münchner Autobauer geht es darum, Transparenz über die gesamte Lieferkette hinweg herzustellen und seine Supply Chain für künftige Herausforderungen fit zu machen.

38 **Wie L'Oréal den E-Commerce ausbaut**
Der Kosmetikkonzern hat im Coronajahr seine Online-Verkäufe deutlich gesteigert. Grundlage dafür: Die Modernisierung der IT-Infrastruktur.

Job & Karriere

40 **Personaler denken nicht digital**
Im Vergleich mit anderen Fachbereichen hinkt „Digital HR" hinterher, so eine aktuelle IDG-Studie. Schlechte Noten kommen von den Fachbereichen, aber auch Personaler sind selbstkritisch.

44 **Die letzte Meile der Digitalisierung**
Tradierte Lernkonzepte stoßen an ihre Grenzen. Neue Tools sollen nun Lernen und Arbeiten verknüpfen und die Digital Adoption der Mitarbeiter fördern.

46 **Pluspunkt Digital-Know-how**
Auf welch unterschiedlichen Wegen man Digital-Qualifikationen aufbauen kann, zeigen die Beispiele einer SAP-Beraterin und des Chemiekonzerns Wacker.

47 **Stellenmarkt**

49 **Impressum**

50 **IT in Zahlen**

Landwirtschaft 4.0 – mit Digitalisierung zu mehr Umweltschutz und Effizienz

Die Zukunftskommission Landwirtschaft fordert radikale Veränderungen im deutschen Agrarsektor. Digitale Techniken könnten eine Schlüsselrolle dabei spielen, die Produktivität zu erhalten und gleichzeitig die Umwelt zu schonen.

Von Martin Bayer,
Deputy Editorial Director

So kann es nicht weitergehen. Das Fazit der Zukunftskommission Landwirtschaft ist eindeutig. „Eine unveränderte Fortführung des heutigen Agrar- und Ernährungssystems scheidet aus ökologischen und tierethischen wie auch aus ökonomischen Gründen aus“, schreiben die Experten in ihrem Abschlussbericht „Zukunft Landwirtschaft“. Sie heben auf der einen Seite die gerade im Zuge von technologischen Fortschritten erzielten Produktionssteigerungen hervor, womit die Bevölkerung immer zuverlässiger und günstiger mir Nahrung versorgt werden könne. Kehrseite dieses Fortschrittes seien jedoch Formen der Übernutzung von Natur und Umwelt, von Tieren und biologischen Kreisläufen bis hin zur gefährlichen Beeinträchtigung des Klimas.

Der allgemeine Fortschritt und die Erweiterung der technischen Möglichkeiten hätten den Strukturwandel der Landwirtschaft rasant beschleunigt, steht in dem Bericht. Dies habe enorme Produktions- und Produktivitätssteigerungen gebracht. Gleichzeitig sei ein Kostendruck entstanden, unter dem immer mehr Familien für ihre Höfe keine Perspektive sehen. „Diese Entwicklungen haben dazu geführt, dass die Landwirtschaft immer weniger in der Lage ist, in ökologisch verträglichen Stoffkreisläufen innerhalb der Belastungsgrenzen der natürlichen Ressourcen zu wirtschaften.“

Präziser arbeiten auf dem Acker

Die Expertenkommission hat eine Reihe von Vorschlägen entwickelt, wie die Landwirtschaft in Zukunft besser funktionieren könnte. Anfang Juli wurde der Abschlussbericht Bundeskanzlerin Merkel offiziell übergeben. Neben

Foto: Leonid Sorokin/Shutterstock

Übernahme von RiskIQ – Microsoft baut sein Security-Portfolio aus

Mit RiskIQ kauft Microsoft Tools für Cyber Threat Intelligence hinzu. Damit sollen Kunden ihre oft heterogen zusammengesetzten Infrastrukturen besser absichern können. Doch auch die Security selbst wird immer komplexer.

IT-Sicherheit ist zu komplex

Viele Unternehmen kämpfen mit ihrer kaum noch beherrschbaren Security-Infrastruktur. Zu dieser Erkenntnis kommt eine Studie, die Fastly, Anbieter einer Edge-Cloud-Plattform, bei der Enterprise Strategy Group (ESG) beauftragt hat. Beispielsweise seien die von den Sicherheitslösungen generierten False Positives ein ebenso großes Problem wie erfolgreiche Angriffe auf die Sicherheit. Fast die Hälfte aller Security-Warnungen seien Fehlalarme, verursacht durch harmlose Geschäftsaktivitäten. 75 Prozent der rund 500 befragten Unternehmen wenden für sie ähnlich viel Zeit auf wie für echte Angriffe, konstatieren die Analysten. Das führe dazu, dass etliche Betriebe ihre Sicherheitslösungen abschalteten oder im Logging- oder Monitoring-Modus laufen ließen.

Es bestehe ein hoher Bedarf an einheitlichen, modernen und vor allem einfachen Sicherheitskonzepten, lautet das Fazit der Analysten. „Sicherheitsexperten sind frustriert über die Komplexität und den isolierten Charakter traditioneller Lösungen für die Anwendungssicherheit, die diesen Anforderungen nicht gerecht werden", sagte John Grady, Senior Analyst bei ESG. „Moderne Unternehmen benötigen einheitliche Tools und Ansätze, die Schwachstellen zwischen ihrer Public-Cloud-Infrastruktur, Microservices-basierten Architekturen und Legacy-Anwendungen minimieren und gleichzeitig eine Vielzahl von Personas unterstützen können."

Mit der Übernahme von RiskIQ weitet Microsoft sein Angebot an Security-Lösungen aus. RiskIQ wurde 2009 gegründet und bietet Software für Cyber Threat Intelligence, Incident Response und das Management von Schwachstellen innerhalb der Unternehmens-IT an. Der in San Francisco beheimatete Security-Spezialist hatte in den vergangenen Jahren diverse Finanzspritzen von verschiedenen Investorengruppen erhalten. Wie viel Microsoft für RiskIQ auf den Tisch legt, wurde nicht bekannt gegeben. Die Nachrichtenagentur Bloomberg spekuliert, der Kaufpreis habe bei 500 Millionen Dollar gelegen.

Eric Doerr, Vice President für den Bereich Cloud Security bei Microsoft, beobachtet, dass Anwenderunternehmen mit einer zunehmenden Raffinesse und Häufigkeit von Cyberangriffen konfrontiert sind. Hinzu komme, dass IT-Infrastrukturen im Zuge der stärkeren Cloud-Nutzung und hybrider Arbeitsszenarien zunehmend heterogen zusammengesetzt seien. „Letztlich ist das Internet das neue Netzwerk", konstatiert der Microsoft-Manager. Für die Verantwortlichen in den Betrieben werde es daher wichtiger, genau zu verstehen, wie ihre IT-Assets in einer hybriden Welt aus eigenen Rechenzentren, verschiedenen Clouds und Edge-Ressourcen zusammenhängen.

Laut Doerr kommt es künftig darauf an, Bedrohungen schneller zu erkennen, um die eigene Angriffsfläche zu reduzieren. Dabei sollen in Zukunft die Lösungen von RiskIQ helfen. Die Tools sammeln beispielsweise globale Bedrohungsdaten, werten diese mithilfe von maschinellem Lernen aus und setzen die so gewonnenen Informationen in Relation mit der jeweiligen Sicherheitsarchitektur des Anwenderunternehmens. Die Betriebe erhielten laufend Indikatoren für potenzielle Bedrohungen und könnten Angriffen vorbeugen und diese bestenfalls neutralisieren, versprechen die Manager von RiskIQ. Security-Verantwortliche könnten die Schwachstellen in ihrer Infrastruktur besser erkennen. Mithilfe von RiskIQ ließen sich Zusammenhänge zwischen der eigenen Angriffsfläche und den aktuellen Aktivitäten von Hackern im Netz herstellen. Auf Basis dieser Daten seien schnelle Reaktionen und damit ein optimaler Schutz möglich. Zu den Kunden von RiskIQ zählen American Express, BMW, BNP Paribas und Facebook. Hinter den Security-Lösungen steht dem Unternehmen zufolge eine Community von mehr als 100.000 Sicherheitsspezialisten und Schwachstellen-Jägern. „RiskIQ hat eine starke Kundenbasis und eine Gemeinschaft von Sicherheitsexperten aufgebaut, die wir weiterhin unterstützen, pflegen und ausbauen werden", kündigte Doerr an. Die Technologie und das Team von RiskIQ würden das Microsoft-eigene Security-Portfolio ideal ergänzen.

Wie genau die RiskIQ-Lösungen eingepasst werden sollen, ist allerdings noch unklar. Der Konzern baut seit geraumer Zeit sein eigenes Produktangebot rund um IT-Sicherheit laufend aus. Neben Tools für die Absicherung von Endgeräten in Microsoft 365 und dem Windows-Betriebssystem offeriert Microsoft verschiedene Lösungen für die Sicherheit seiner eigenen Cloud wie zum Beispiel „Azure Sentinel" für das Security Incident Event Management (SIEM) oder „Insider Risk Management", um Bedrohungssignale zu sammeln und hinsichtlich ihres Gefahrenpotenzials auszuwerten. Diese Funktionen ähneln den Tools von RiskIQ. Hier dürfte an der einen oder anderen Stelle sicherlich eine Bereinigung des Tool- und Funktionsumfangs anstehen. *(ba)*