CLOUD-SECURITY ERFORDERT UMDENKEN

Wie kann IT-Security im Zeitalter von Cloud, Hybrid Cloud und Multi-Cloud aussehen? Über diese Frage hat die COMPUTERWELT im Rahmen eines Round Tables mit sieben heimischen Experten diskutiert..

Die Cloud, vor einigen Jahren noch für viele unvorstellbar, ist heute als Technologie akzeptierte und gelebte Realität, wird aber auch kritisch hinterfragt. Daten, Anwendungen und Teile der eigenen IT-Infrastruktur an einen oder mehrere externe Provider auszulagern – davor haben viele Unternehmen nach wie vor noch Angst. IT-Security wird dabei einerseits als Pro- als auch als Contra-Cloud-Argument von Entscheidern genannt, wie es auch im neuesten Cloud Security Report 2019 von IDG nachzulesen ist. Für Cloud-Services sprechen bei den Befragten vor allem eine standardisierte IT und eine orts-, geräte- und ressourcenunabhängige Nutzung. Als Gegenargumente werden Sicherheitsbedenken und Datenschutzgründe genannt. Besonders interessant: Die beiden meistgenannten Contra-Argumente sind auch auf der Pro-Seite unter den Top-fünf-Argumenten.

Irene Marx, seit kurzem beim Cloud Spezialisten Zscaler verantwortlich für die Region Österreich/Schweiz meint zur heutigen Situation: »Ich glaube nicht, dass Unternehmen heute vor der Entscheidung stehen, ob sie in die Cloud gehen oder nicht. Es geht eindeutig dorthin.« In einer jüngst von Zscaler durchgeführte Umfrage mit 400 Entscheidungsträgern wurde aufgezeigt, dass bereits acht Prozent der befragten Unternehmen ihre Transformation in die Cloud abgeschlossen haben. Weitere 26 Prozent der Unternehmer planen im kommenden Jahr, 100 Prozent ihrer Applikationen in die Cloud zu geben. Damit steht für Marx fest: »Man kommt heute ohnehin nicht um die Cloud herum. Daher muss man natürlich den Datenverkehr in die Cloud absichern und die Cloud selbst auch. Die großen Herausforderungen liegen darüber hinaus in der Performance und User Experience.«

Stefan Schachinger, Product Manager für CloudGen Firewall bei Barracuda Networks, hat eine ähnliche Sichtweise: »Ja, die Reise in Richtung Cloud hat eindeutig schon eingesetzt und wird auch nicht aufhören. Ich würde aber nicht behaupten, dass die Cloud per se sicher oder unsicher ist. Man muss sich darum einfach nur kümmern.« Schachinger sieht heute Unternehmen allerdings in der Komplexität mehr gefordert als früher: »Unternehmen öffnen sich nach außen, in dem auch andere Standorte und Services angebunden werden, auf die man ja irgendwie zugreifen muss. Das wird in vielen Fällen über das Web passieren. Dabei ist aber auch die entsprechende Performance ein großes Thema, damit die Applikationen auch aus der Ferne für User verwendbar bleiben.«

Christine Wahlmüller (vorne links) hat mit sieben heimischen Experten über Cloud-Security diskutiert.

SHARED RESPONSIBILITY

Gedanken machen sollte man sich auch über das Thema Shared Responsibility: »Der Cloud-Anbieter kümmert sich um die Sicherheit der Infrastruktur, sorgt dafür, dass die Rechenzentren entsprechend abgesichert sind – und der Endkunde ist für die Sicherheit der Applikationen und der Daten selbst verantwortlich.« Genau hier liegt Schachinger zufolge eine große Herausforderung für viele Unternehmen.

AUF DIE PROZESSE KOMMT ES AN

Tim Berghoff, IT-Security Evengelist bei G Data, einem deutschen IT-Security-Unternehmen, das seine Wurzeln im Bereich Endpunkt-Absicherung hat, sieht IT-Security in der Cloud-Ära als komplexe Aufgabe: »Was wir in den letzten Jahren bemerkt haben, ist, dass IT-Security ein sehr stark prozessgetriebenes Business ist. Da müssen wir uns mittlerweile aufgrund der Tatsache, dass sich Firmennetzwerke immer weiter öffnen, mehr Gedanken machen. Gerade beim Thema Cloud ist es ganz entscheidend, handlungsfähig zu bleiben, wenn es wirklich zu einem Sicherheitsvorfall kommt. Da wird aus Sicht der IT-Sicherheit in Zukunft ein großer Teil der Marschrichtung hingehen.«

Leopold Obermeier, Cloud- und IT-Security-Experte bei Fujitsu Österreich, sieht die Themen Cloud und IT-Security untrennbar

miteinander verbunden: »Wir verfolgen einen Multi-Cloud-Ansatz, wir sehen uns als Partner von allen Hyperscalern und versuchen hier, eine End-to-End-Betrachtung anzustellen. Es geht darum, die Security zwischen den einzelnen Cloud-Systemen abzusichern. Heute geht es Richtung Daten-Security und weg von einer Device-Security, die lange Zeit favorisiert wurde.« Obermeier ist auch Vortragender der FH Burgenland und zudem bei EuroCloud Austria engagiert im Einsatz: »Mit dem Star Audit bietet EuroCloud eine Zertifizierung für Cloud-Systeme. Es wird aktuell in der Version vier um eine Control Area sieben erweitert, die sich mit dem Thema Data Protection beschäftigt und 30 Kontrolloptionen beinhaltet.« Ziel und Zweck des Star Audits ist es, durch einen transparenten und verlässlichen Zertifizierungsprozess eine nachvollziehbare Qualitätsbewertung von Cloud-Diensten zu ermöglichen.

GESAMTHEITLICHE SICHTWEISE NÖTIG

Ebenso bei der Expertenrunde mit dabei war Martin Madlo, Managing Direktor von Interxion Österreich. Das Unternehmen beschäftigt sich seit rund 20 Jahren mit Colocation Services und betreibt in Österreich einen Rechenzentrumscampus in Wien Floridsdorf, der erst letzten Herbst mit einem großen Zubau erweitert wurde. »Wir betreiben über 50 Rechenzentren in ganz Europa und natürlich ist das Thema Security eines, das uns seit vielen Jahren begleitet«, betont Madlo. »Ich würde das Thema nicht darauf reduzieren wie sicher oder unsicher die Cloud ist. So wie bei vielen anderen Themen vor der Cloud muss IT-Security im Unternehmen ein gesamtheitliches Konzept sein, das alle Parameter der handelnden Personen, der im Netzwerk befindlichen Komponenten einbezieht. Und genauso muss IT-Security auch jetzt bei Hypercloud-Anwendungen oder bei Einbindung von IoT gehandhabt werden. Es darf keine singuläre Betrachtungsweise sein, sondern wichtig ist ein Gesamtkonzept inklusive Maßnahmen für den Notfall.« Interxion arbeite mit sehr vielen Cloud-Anbietern zusammen, »und die Maßnahmen, die von diesen Anbietern getroffen werden, um ihren Teil der Arbeit sauber abzuwickeln, sind enorm. Ich glaube, da können auch viele Unternehmen sehr viel davon lernen, welche Prozesse hier implementiert worden sind, welche Maßnahmen auch von den Zulieferern dieser Service-Provider gefordert werden, um die Cloud sicher zu machen. Die Cloud-Service-Anbieter sind sich sehr wohl der Tatsache bewusst, dass die Daten ihrer Kunden das wichtigste Gut sind, das sie verwalten.«

DIE RICHTIGE ARCHITEKTUR

Daniel Tremmel, Security Solutions Architect bei A1 Digital, warnt vor Schnellschüssen: »Wir beschäftigten uns derzeit sehr stark mit Enterprise Security Architektur. Wir sehen im Bereich Cloud, dass technisch sehr vieles schnell realisiert werden kann, oftmals ohne dass im Unternehmen gewisse Stellen etwas davon mitbekommen. Aber es geht schon darum, dass man das sowohl von der Architektur als auch in punkto Security richtig abbildet und im Unternehmen sicherstellt, dass gewisse Voraussetzungen oder Bedingungen erfüllt sind.« Unternehmen rät er bei der Entscheidung für die Cloud vor allem auch darauf zu achten, dass der Weg in die Cloud sicher ist. »Heute darf Security kein Beiwerk mehr sein, sondern muss überall in den Services und in den Funktionen, die wir in der Cloud deployen, vorhanden sein. Man muss sich ja nur ansehen, was alles in letzter Zeit passiert ist. Es ist daher ganz wichtig, Security von Anfang an überall mitzudenken und einzusetzen. Das ist die einzige Möglichkeit, wie man als Unternehmen in die Cloud gehen kann. Das erfordert sicher eine Änderung des Mindsets aber wir brauchen heute einen gewissen Security Standard.«

Wolfgang Zuser, langjähriger Projektmanager von Security-Projekten bei Antares NetlogiX, einem IT-Security-Dienstleister aus Amstetten, nennt drei Aspekte: »Ein Projektmanager beschäftigt sich viele, viele Tage im Jahr damit, einerseits den Kampf gegen Viren und Cyber-Attacken von der Theorie in die Praxis in eine technisch brauchbare Abwehr zu»übersetzen. Das zweite große Thema ist die ständige Abwägung zwischen Verfügbarkeit und IT-Security.« Antares NetlogiX kennt IT-Security seit kurzem auch aus einem anderen Blickwinkel: Das Unternehmen ist heute selbst als Cloud-Anbieter tätig. »Dritter großer Aspekt ist sicher der menschliche Faktor, einerseits in der Anwendung und Umsetzung aller Security-Richtlinien und Best Practices, die es gibt, aber auch in der technischen Gestaltung eines Gewerks, wo bestimmte Personen mit unterschiedlichen fachlichen Hintergründen und Spezialistenwissen aufeinandertreffen und unterschiedliche Denkweisen einbringen, die es dann abzugleichen gilt.«

Tim Berghoff, G Data: »Dankenswerterweise ist der Riesen-Hype, dass die Cloud das Allheilmittel für alles ist, nun ein bisschen abgeflacht.«

ZUERST DAS RICHTIGE MINDSET

Was sind nun die großen Herausforderungen für Unternehmen angesichts neuer Technologien wie Cloud, KI, IoT oder Mobility? Wo hakt es und wie können Lösungen aussehen? Daniel Tremmel von A1 Digital: »Gerade Cloud ist ja in den letzten Jahren in aller Munde. Man muss aber ehrlich sagen: Die Probleme waren eigentlich immer schon dieselben: Einerseits geht es darum, das Wissen in das Unternehmen zu bringen und die Ser-

vices richtig anzubinden. Technisch geht das ganz schnell, aber die Frage ist: Wie gut und richtig ist die Anbindung, wie sind organisatorische Fragen gelöst etc.? Man muss die Sichtweise auch sehr stark in Richtung organisatorischer Fragen verlagern: Prozesse ansehen, für die Mitarbeiterausbildung mit Schulungen und Trainings sorgen. Es ist ganz wichtig, die Mitarbeiter abzuholen und ihnen zu vermitteln, was es denn bedeutet, in die Cloud zu gehen. Erst im nächsten Schritt, wenn das Mindset da ist, sollte man dann die technische Umsetzung angehen, die Anbieter vergleichen, Angebote einholen und schauen, wie man die Anforderungen am besten technisch lösen könnte«, rät Tremmel.

ORGANISATORISCHE HERAUSFORDERUNG

Auch Tim Berghoff sieht das ähnlich: »Gerade im KMU-Bereich haben wir es mit historisch gewachsenen Strukturen zu tun, sowohl auf der technischen Seite in der IT, als auch in den Köpfen. Demgegenüber steht die Realität, die wir jetzt haben, und die nennt sich nun mal Cloud. Dankenswerterweise ist der Riesenhype, dass die Cloud das Allheilmittel und der Segensbringer für alles ist, nun abgeflacht, sodass man nun beginnt, sich ernsthaft mit dieser Technologie auseinandersetzen und sich überlegt: Wo kann man die Technologie sinnstiftend einsetzen und welche Änderungen sind dafür sowohl auf der technischen als auch auf der organisatorischen Seite notwendig.« Für Berghoff reicht die Palette der Maßnahmen von Mitarbeiterschulungen bis dahin, radikal die Konzepte zu überdenken, die jetzt eingesetzt werden. »Viele haben leider die Mentalität: wenn es nicht kaputt ist, repariere ich es auch nicht.«

Das ist ein gefährliches Denken, warnt auch Barracuda Experte Schachinger: »Security muss natürlich gelebt werden. Wenn ein System zehn Jahre funktioniert, bedeutet das noch lange nicht, dass es auch sicher ist. Darüber hinaus muss sich jeder Betrieb natürlich Gedanken machen, welche der neuen Technologien Sinn machen. Gerade was die Cloud betrifft werden sich die meisten in einer hybriden Umgebung wiederfinden. Ganz wenige werden in Zukunft alles lokal betreiben und es wird auch ganz wenige geben, die alles in die Cloud schieben. Für die meisten bestehenden Unternehmen wird es so sein, dass einige Teile lokal und andere Teile ausgelagert sind. Die Cloud-Anbieter sind sich

Martin Madlo, Interxion: »IT-Security muss im Unternehmen ein gesamtheitliches Konzept sein, das alle Parameter berücksichtigt.«

natürlich bewusst, dass sie Einiges zu verlieren haben, nicht nur Daten, sondern auch Reputation. Große Anbieter wie Microsoft oder AWS ziehen natürlich mehr Aufmerksamkeit auf sich als der klassische österreichische Mittelständler. Das wissen die aber auch und kümmern sich dafür intensiver um ihre Kunden.«

BASIS-SECURITY MUSS STIMMEN

Eine Gefahr sieht Martin Madlo darin, »dass sich Unternehmen für gewisse IT-Security-Themen sehr stark interessieren, etwa für die Frage: Wie sicher kann ich meine Cloud machen? Aber die Hausaufgaben wie ein sorgfältiges Patch-Management werden vernachlässigt oder völlig außer Acht gelassen. Hier sollte viel mehr Bewusstsein geschaffen werden, dass es da Basis-Security-Standards gibt, die ich als Unternehmen erst einmal erreichen muss.« Dieser Aussage stimmen auch die übrigen Teilnehmer des Round Tables zu und formulieren gemeinsam folgende dringende Empfehlungen an Unternehmen: Gelebte IT-Security heißt, die Mitarbeiter entsprechend zu schulen und notwendige Standard-IT-Security-Maßnahmen wie etwa regelmäßiges Patching durchzuführen bzw. notwendige Patch-Prozesse zu definieren.

Die Verantwortung bei IT-Security hat sich etwas gewandelt, stellt Wolfgang Zuser fest: »Früher war IT-Security vor allem auf Netzwerk und Firewalling beschränkt. Aufgaben wie Patch-Management und Passwort-Management konnte man, auch mit etwas Glück, ein wenig vernachlässigen, solange die Sicherheitsmaßnahmen am Perimeter zuverlässig funktionierten. Das ist in der Cloud natürlich anders. Cloud-Management-Zugänge wie etwa bei MS Azure sind exponiert, schlechtes Passwort Management und schlechte Passwortwahl können fatale Auswirkungen haben. Daher gilt es, die Security Awareness zu erhöhen und das Thema IT-Security im Unternehmen anders, heißt ganzheitlich, zu organisieren. Wir müssen heraus aus dem Netzwerkdenken und hinein in alle technischen Facetten.« Als zweites wichtiges Thema nennt Wolfgang Zuser das Thema Prozesse: »Wir können die Prozesse nicht mehr alleine handhaben, sondern müssen mit den Cloud-Anbietern interagieren.«

MEHR SECURITY-AWARENESS MUSS HER

Auch Irene Marx plädiert für ein Umdenken: »Das alte Denken, ich habe hier mein Unternehmen, rundherum habe ich Firewalls und draußen ist das böse Internet – das ist einfach passé! Die Realität schaut anders aus: die Mitarbeiter greifen auf Unternehmensdaten von extern bzw. unterwegs zu, ob das in einem Café oder in einem anderen Unternehmen ist, ob am Flughafen, in unterschiedlichen Niederlassungen oder wo auch immer. Da braucht es eine Strategie um die Daten sicher und verlässlich zur Verfügung zu stellen und vor allem den harten Kern der Unternehmensdaten zu schützen. Für den User selbst ist es ja dabei egal, wo die Daten liegen, ob in der Cloud oder lokal im Datencenter.« Ihr Rat an Unternehmen: »Ganz wichtig ist, bevor man Daten in die Cloud

schiebt oder Office365 ins Auge fasst: Zuerst einen Schritt zurück machen, Netzwerk-ready werden und darauf achten, dass man die entsprechende Performance hat. Es geht darum, vorher die notwendige Infrastruktur zu haben. Weil sonst passiert es, dass User nicht zugreifen können, oder es dauert gefühlt ewig, bis sie via VPN Zugang zu den Daten haben.«

IOT SORGT FÜR NEUE PROBLEME

Leo Obermeier sieht die Vorgangsweise vieler Firmen auch hinsichtlich Usablity kritisch: »Viele Unternehmen, etwa im Bankensektor, haben einfach vor zehn Jahren das User Interface an ihre Endkunden ausgelagert – und so sah das Telebanking früher auch aus. Durch den Zugriff auf Applikationen von viel mehr Usern und vor allem nicht-IT-affinen Leuten ergeben sich ganz andere Angriffsmöglichkeiten. In Wahrheit ist Online Banking nichts anderes als ein Cloud-Angebot, das wir alle schon seit vielen Jahren nutzen, ohne von Cloud zu reden.« Heute drehe es sich aber nicht nur um IT-Infrastruktur und Applikationen, sondern auch das Thema IoT bringe erhebliche IT-Security Risiken mit sich, warnt Obermeier: »Beispiel Therme: Heute wird die vernetzte Therme installiert. So haben wir auf einmal 20.000 Thermen von einem bestimmten Hersteller, wo überall mit dem gleichen Passwort zugegriffen werden kann, weil die Leute, die das Gerät installieren, das vom Hersteller gesetzte Passwort aus Unwissenheit einfach nicht ändern. Da ist dringend Aufklärungsarbeit notwendig.« IoT-Security sei überhaupt ein eigenes Thema: »Wir haben an der FH Burgenland dazu ein eigenes Forschungsfeld, wo man jetzt auch auf neue Themen stößt. Zum Beispiel kostet die Verschlüsselung viel Energie bzw. viel Rechenleistung.«

Zum Thema IoT ergänzt Daniel Tremmel: »Es ist natürlich ganz etwas anderes wenn man Züge und Baumaschinen mit Sensoren ausstattet. Da geht es um Akkulaufzeiten von fünf, sechs Jahren, also einen sehr geringen Energieverbrach.« Natürlich gehe es aber gerade beim Thema IoT darum, nicht auf IT-Security zu vergessen: »In welchem Bereich ist es eingesetzt, wo ist das Gerät angebunden, welche Daten werden da erhoben, sind das sensible Daten und wie ist da die Angriffsfläche bzw. wie kann der Angreifer auf diese Daten kommen? Etwa wenn er sich das Gerät schnappt und irgendwo ansteckt? Das sollte man alles schon bei der Entwicklung des Geräts bedenken. Hier IT-Security abzuwägen ist natürlich schon viel schwieriger als in einem klassischen Client-/Server-Umfeld.«

SECURITY ALS LAUFENDER PROZESS

Das wichtigste Schlagwort im Cloud-Umfeld ist aus Tremmels Sicht Veränderung: »Viele glauben: Ich baue mir meine Cloud und dazu meine Sicherheits-Controls. Und wenn das gebaut ist, dann ist es sicher und dann lasse ich es fünf Jahre laufen. Viele stecken da noch in dieser klassischen Denkweise eines Datacenters vor zehn Jahren. Einmalig Maßnahmen zu setzen, ist heute zu wenig. Es geht um genaue Dokumentation, kontinuierli-

Irene Marx, Zscaler: »Der Druck auf die IT wächst, den Usern Commodity und eine gute User Experience zu verschaffen.«

ches Monitoring und ständige Updates bzw. Verbesserungen. Man muss schauen: Gibt es neue Geräte, neue Angriffsflächen, neue Bedrohungen, gibt es neue Patches, die man einspielen muss etc.? Das sollte ein kontinuierlicher Prozess sein, der ständig und möglichst automatisiert abläuft, sowohl in der Cloud als auch im eigenen Datacenter.«

GUTES TERRAIN FÜR SECURITY-DIENSTLEISTER

Tim Berghoff bemerkt, dass es gerade im KMU-Bereich vielfach an notwendigem Wissen fehlt: »Da bekommen Leute Anforderungen, Dinge zu konfigurieren und abzusichern, die sie mit ihrem Wissensstand so nicht leisten können oder nur mit einem wirtschaftlich nicht mehr vertretbaren Aufwand.« Er prognostiziert, dass sich ein spezialisierter IT-Security-Dienstleistungsbereich stark entwickeln wird: »Das wird dazu führen, dass bestimmte Prozesse automatisiert sind, weil einfach diese Flut an Daten, die von Sensoren draußen im Feld kommen, sich von einer Gruppe von Menschen gar nicht mehr sinnvoll verarbeiten lassen. Automatisierung wird eine Menge an Arbeit erleichtern, dafür entsteht mehr Bedarf und Arbeit in punkto IT-Security.«
Die theoretischen Security-Konzepte sind in der Praxis oft einfach nicht anwendbar, sieht Wolfgang Zuser die Unternehmen heute gefordert, Krisenbewältigung und eine »Was passiert wenn«-Strategie zu entwickeln: »Das Thema reaktive Maßnahmen gewinnt heute sicher stark an Bedeutung. Hier ist mitloggen wichtig. Sollte tatsächlich etwas passieren, müssen die Unternehmen schnell darauf reagieren können. Leider ist dieses Thema in vielen Unternehmen heute echt unterversorgt.«

UMDENKEN IST NOTWENDIG

Hier muss ein Umdenken her, fordert Martin Madlo die Unternehmen auf: »IT-Security muss ein Management Cycle sein, mit einer genauen Abfolge von Maßnahmen. Und was ganz wichtig ist: Das Unternehmen muss wirklich eine Risiko-Analyse machen, genauso wie vor 20 Jahren zum Thema Internet und IT-Security. Das heißt: Wo sind meine größten Vulnerabilities und wie kann ich diese adressieren bzw. mich schützen. Mit Blick auf die Usability, damit wir nicht Maßnahmen implementieren, wo ich von vornherein schon annehmen kann, dass sie nicht

Leopold Obermeier, Fujitsu: »Es geht heute darum, die Security zwischen den einzelnen Cloud-Systemen abzusichern und Richtung Daten-Security.«

akzeptiert werden und dass die User versuchen, sie zu umgehen. Der Klassiker dabei ist: Das Passwort wird auf der Tastatur aufgeschrieben. Zusammenfassend heißt das: Wie groß ist mein Risiko in welchem Bereich? Welche technischen und organisatorischen Maßnahmen muss ein Unternehmen setzen, um diese Risiken zu vermindern. Vermeiden kann man sie in vielen Fällen jedenfalls nicht.«

IT-SECURITY SOLL NICHT NERVEN

»Dazu gehört sicher auch die Klassifizierung der Daten«, sagt Leo Obermeier. Das ist ein Thema, das zwar von den großen Unternehmen erkannt und auch gemacht werde, »aber bei den klassischen österreichischen Mittelständlern wird das stark vernachlässigt«. Bezüglich Usability schildert Leo Obermeier seine eigene Erfahrung: »Unsere Remote-Lösung bei Fujitsu zwingt mich, alle 60 Tage einen neuen sechsstelligen PIN-Code einzugeben. Das nervt, das ist keine Usability. Da müssen wir noch andere, bessere Authentifizierungsverfahren einsetzen, zum Beispiel biometrische Verfahren. Es geht darum zu vereinfachen und gleichzeitig Sicherheit zu gewährleisten.«
»Heute erwarten sich die User, dass die IT einfach friktionsfrei funktioniert. Das heißt, der Druck auf die IT wächst, dem User Commodity und eine gute User Experience zu verschaffen«, fügt Irene Marx hinzu.

BENUTZERFREUNDLICHKEIT SPIELT EINE ENTSCHEIDENDE ROLLE

»Benutzerfreundlichkeit ist sehr wichtig, weil man weiß, dass die User sonst die Sicherheitsmaßnahmen umgehen werden«, meint auch Stefan Schachinger. Beim Thema IoT sieht er noch ganz andere Herausforderungen: »Zum einen geht es wieder um die Benutzerfreundlichkeit, denn im IoT-Umfeld hat man es mit Betriebstechnikern oder Elektrikern zu tun, von denen man nicht erwarten kann, dass sie Security-Lösungen durchkonfigurieren können.« Passieren kann jedenfalls jede Menge: Produktionshallen, wo plötzlich die Maschinen stillstehen oder Supermärkte, wo Kühltruhen und Heizung ausfallen. »Hinzu kommt, dass wir es mit Geräten zu tun haben, die nicht dem Sicherheitsniveau der Office-IT entsprechen: Das Patch-Management hinkt hinterher, wir haben keine Antivirus-Lösungen, die installiert werden etc. Daher gilt es, die Geräte umso besser abzuschotten. Umgekehrt müssen sie aber mit der Cloud kommunizieren. Gerade zum Datensammeln und Analysieren bietet sich die Cloud an, weil man da die Rechenpower hat, um sinnvolle Muster herauszusuchen.«
Dabei dürfe man aber nicht auf die IT-Security vergessen, mahnt Wolfgang Zuser und sieht eine Tendenz: »Das Thema Multifaktor-Authentifizierung gewinnt durch die Cloud massiv an Bedeutung.«
Tim Berghoff hakt bei Industrial IoT ein: »Wir haben ein Riesenproblem eben aufgrund der Tatsache, dass man da Maschinensysteme stehen hat, die meist nur einmal pro Jahr heruntergefahren werden. Da wird dann

COMPUTERWELT

Jetzt kostenlos testen!

Testen Sie jetzt

10 Ausgaben

und schicken Sie

ein E-Mail mit dem

Kennwort TEST 10 an

abo@cwverlag.at

Bitte geben Sie im E-Mail Ihren Vor- und Zunamen und die Zustelladresse an.
Wenn Sie die COMPUTERWELT in Ihre Firma wollen, geben Sie bitte zu Ihrem Namen auch den Firmennamen und die Firmenadresse an.

Dieses Angebot gilt bis 31. Dezember 2019 und ist nur gültig sofern in den letzten 6 Monaten kein kostenloses Probeabo bezogen wurde. Probeabo kann nicht auf bestehende Abos angerechnet werden. Das Probeabo endet automatisch.

alles an Wartungsarbeiten in dieses eine Wartungsfenster hineingelegt und den Rest des Jahres passiert nichts. Im schlimmsten Fall bekommt auch gar niemand etwas mit, wenn auf so einem System irgendjemand et-

Stefan Schachinger, Barracuda: »Die Cloud ist nicht per se sicher oder unsicher. Man muss sich darum einfach nur kümmern.«

was anstellt. Die Frage ist aber, von wo wird das Bedürfnis nach Sicherheit denn getrieben? Von der eigenen IT-Abteilung oder von außen, etwa durch eine Compliance Abteilung? Das Schöne ist, dass aus meiner Sicht gerade ein Generationenwechsel im Gange ist, wo neue Administratoren nachrücken, die anders denken und vielleicht mehr bereit sind, neue Ansätze auszuprobieren.« Es sei alles auch immer ein wenig ein zweischneidiges Schwert: »Das Schöne bei Cloud ist ja: Man gibt Verantwortung ab. Der Nachteil ist aber auch: Man gibt Verantwortung ab.«

SCHLECHTE PASSWÖRTER ALS SECURITY-DAUERBRENNER

Schlechte, unsichere Passwörter sind nach wie vor eines der großen Security-Probleme. Daniel Tremmel sieht hier einen Trend: »Der Passwortwechsel alle 50, 60 Tage ist absolut nicht mehr zeitgemäß, weil die User immer Wege finden, wie sie solche Sicherheitsmaßnahmen umgehen. Es geht mehr in Richtung Multifaktor-Authentifizierung, es geht mehr um Absicherung der Zugänge. Es braucht heute vor allem eine ganzheitliche Sicht der Dinge, eine ganzheitliche IT-Security, weil es gibt immer irgendeine Schwachstelle oder ein Gerät und genau da passiert dann etwas. Und so kann der Angreifer eine komplette Security aushebeln.«

Tim Berghoff sieht das klare Bekenntnis des Top-Managements zu IT-Security als ganz wichtigen Punkt: »Wenn es von der Geschäftsleitung unterstützt und umgesetzt wird, hat das ein ganz anderes Gewicht, als wenn es nur von der Fachabteilung kommt.« Aber auch das Mindset der Mitarbeiter spiele natürlich eine große Rolle: »Die jungen Teams, die Startups, die IT-Abteilungen oder Entwickler, DevOps und DevSecOps – daraus wird der neue Zugang zu IT-Security getrieben. Da gibt es die Agilität, die schnellen Prozesse und Abläufe, dass man auch dementsprechend schnell reagieren kann.«

Ein Security Patentrezept gibt es allerdings nicht, meint Martin Madlo: »Das Spannende ist, dass es keine IT-Security gibt, die über alle Unternehmen replizierbar ist. Stattdessen müssen sich Unternehmen die Frage stellen: Woher kommt denn die Bedrohung? Ein Industrie-Unternehmen, das stark in der Forschung und Entwicklung ist, wird sicher andere Themen haben in Richtung Industrie-Spionage, wo hoch bezahlte kriminelle Energie dahintersteckt. Da werden die Maßnahmen ganz anders aussehen als bei einem Unternehmen im öffentlichen Bereich, wo Denial-of-Service-Attacken im Vordergrund stehen. Die Frage ist: was ist es einem potenziellen Angreifer wert, die IT-Securitiy eines bestimmten Unternehmens zu überbrücken? Und was ist es diesem Unternehmen wert, sowohl organisatorische als auch technische Maßnahmen zu implementieren, oft begleitet von externen Experten, um es einem potentiellen Angreifer so teuer und schwierig wie möglich zu machen?«

VERNETZUNG UND MIKRO-SEGMENTIERUNG

Gerade um es den Angreifern schwierig zu machen, gibt es ja viele technische Möglichkeiten. »Eine gute Möglichkeit ist sicher Mikro-Segmentierung. Da geht es darum, die einzelnen Bereiche voneinander zu trennen und abzusichern. Das gilt insbesondere für das OT-Umfeld. Mikro-Segmentierung wird

Daniel Tremmel, A1 Digital: »Es ist ganz wichtig, Security von Anfang an überall mitzudenken. Nur so kann man als Unternehmen in die Cloud gehen.«

in dem Zusammenhang immer wichtiger, weil die IT sich über alle Fachabteilungen hin ausbreitet«, betont Irene Marx.

Ein großes Problem ist hier genau die zunehmende Vernetzung »und, dass plötzlich Maschinen, die vor zehn Jahren angeschafft worden sind, jetzt auf einmal reden«, stellt Stefan Schachinger fest. Hinzu kommt das heute oft fehlende oder abhanden kommende Wissen zu den Maschinen: »Es kann ja sein, dass der Hersteller einer Maschine überhaupt nicht mehr vorhanden ist. Da gibt es Maschinen, die sind 20 Jahre oder mehr im Einsatz«, fügt Leo Obermeier hinzu und schildert eine weitere Herausforderung: »Wir haben auch bei den DB-Servern im Zuge von Meltdown und Spectre jetzt ein großes Problem: wir können da nicht patchen, weil die Patches so viele Perfomance-Einbußen bringen. Daher muss ich das System im Vorfeld so isolieren, dass wirklich

nur noch das zum System hinkommt, was valide ist.«

IT-SECURITY STRATEGIE UND AUSBLICK

Viele Problemfelder und Herausforderungen wurden aufgeworfen, aber was können nun Unternehmen konkret tun, um im Cloud-Zeitalter ihre Unternehmens-IT, Applikationen und vor allem Daten zu sichern? »Es ist vor allem einmal wichtig, überhaupt einmal eine IT-Security-Strategie zu haben und diese dann methodisch korrekt aufzusetzen«, rät Wolfgang Zuser und weiter: »Dazu gehören natürlich Business- und Risikoanalysen, technische Grundlagen und all die Aspekte, die in der Cloud neu sind. Und wenn die Hausaufgaben gemacht sind, kann man davon auch eine Strategie ableiten, die zumindest einige Jahre in die Zukunft reicht. Wir sind am Anfang des Weges in die Cloud aber da ist noch ein weiter Weg zurückzulegen.«
Etwas anderer Meinung ist Martin Madlo: »Ich widerspreche der Aussage, dass man nicht sehr weit in die Zukunft blicken kann. Wenn man als Unternehmen diese Management-Struktur schafft, um IT-Security zu implementieren, dann ist das sehr losgelöst von der Technologie, die letztendlich verwendet wird. Grundsätzliches wie die Prozesse und dass IT-Security ganz oben im Management angesiedelt werden und von dort unterstützt werden muss, das ändert sich eigentlich auch nicht durch Cloud, IoT oder irgendwelche zukünftigen Technologien.«

KONTINUIERLICHE SCHULUNG DER MITARBEITER

Zu bedenken sind trotzdem die schnellen Veränderungen, die auch rasche Anpassungen notwendig machen. Daniel Tremmel rät: »Man muss ein bisschen Dynamik hereinbekommen. Das heißt: Auch Entscheidungen, die jetzt gefällt werden, sollten in sechs Monaten oder einem Jahr auch noch Gültigkeit haben, und man muss nicht wieder bei Null anfangen. Ich glaube, wir sind da schon in die richtige Richtung unterwegs, auch von den Skills und vom Mindset bei Mitarbeitern und Entscheidern. Es ist aber noch ein etwas längerer Weg in punkto IT-Security wirklich eine länger währende, spürbare Verbesserung zu erreichen. Kontinuierliche Mitarbeiterschulung ist jedenfalls wichtig.«
Stefan Schachinger bringt neben dem menschlichen Faktor und User Awareness noch einige weitere Punkte ein: »Security ist

Wolfgang Zuser, Antares NetlogiX: »Es gilt, die Security-Awareness zu erhöhen und das Thema IT-Security ganzheitlich zu organisieren.«

auch immer untrennbar mit Connectivity verbunden. Wenn man für sichere Verbindungen sorgt, hat man schon einiges erledigt. Dabei geht es nicht nur um Daten-Verschlüsselung, sondern auch um Einschränkungen auf legitime Applikationen und Protokolle sowie die Erkennung von bösartigen Aktivitäten. Security ist heute einfach mehr als eine Firewall: Es geht um Benutzerrechte und Multifaktor-Authentifizierung. Es geht darum, es mitzukriegen und möglichst früh draufzukommen, wenn und wann etwas passiert ist, damit der Incident Response möglichst rasch bzw. optimalerweise noch während des Vorfalls eingreifen kann. Das größte Einfallstor für Angriffe auf den User ist übrigens nach wie vor E-Mail, mittlerweile gibt es schon sehr gut gemachte Phishing-Attacken. Ein weiteres Thema, das oft stiefmütterlich behandelt wird, ist das Backup. Die Security-Risiken sind da eigentlich die gleichen, egal ob die Daten lokal oder in der Cloud liegen.«

AUF ZERTIFIZIERUNGEN ACHTEN

Sinnvoll sind auch IT-Security Standards bzw. Zertifizierungen, die von Cloud Anbietern und Dienstleistern, aber auch Partnern und Kunden erworben werden können. Erwähnt wurden etwa ISO27001, die Norm zur Zertifizierung von Informations-Sicherheits-Management-Systemen (ISMS) und PCI-DSS (Payment Card Industry Data Security Standard) im Finanzbereich. »Man sollte darauf achten, ob die Partner oder Zulieferer diese Standards auch haben bzw. danach seine Partner auswählen«, rät Wolfgang Zuser.

WAS IST SECURITY WERT?

Eines ist allen Beteiligten klar: Wenn es um Security-Konzepte und -Maßnahmen geht, gehört viel Fachwissen dazu. »Bei vielen Unternehmen ist da ein wenig Abwehrhaltung da, denn IT-Security verursacht natürlich Kosten. Da ist oft die Frage: Kann ich es mir als Unternehmer leisten, so eine Dienstleistung zu kaufen? Die Gegenfrage lautet: Kann es sich ein Unternehmen leisten, es nicht zu machen und es einfach darauf ankommen zu lassen? Klar ist: IT-Security bringt das Kernbusiness nicht so wirklich weiter. Oder anders gesagt: Keiner verkauft mehr Waren, nur weil er ein tolles Sicherheitskonzept hat. Da müssen wir als Hersteller den Unternehmen gegenüber sicher noch mehr und vernünftig argumentieren, warum bestimmte Maßnahmen sinnvoll sind«, ist Tim Berghoff überzeugt.
»Obwohl jetzt auch viel allgemein über IT-Security gesprochen wurde, geht es darum, schon ein eigenes Security-Konzept zu haben, das für die Cloud ausgerichtet ist. Wichtig ist auch, und das kann man nicht oft genug sagen, regelmäßig Mitarbeiter-Schulungen durchzuführen, eine positive User Experience zu schaffen und auf eine gute Usability zu achten. Wenn aber so viel wie möglich von der Technik abgefedert werden kann, unterstützt das das Leben aller Unternehmen und auch deren Mitarbeiter«, stellt Irene Marx abschließend fest. **| CHRISTINE WAHLMÜLLER**