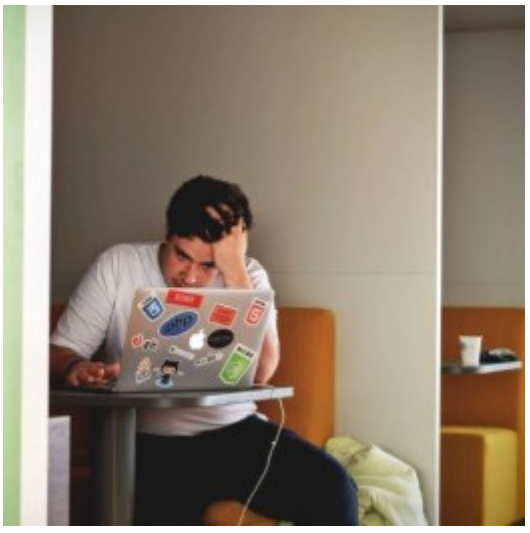
ENTERPRISE (/artikel/enterprise) #SECURITY (/artikel/security)

it&t business Roundtable IT-Security

Steigende Cyberangriffe, steigende Herausforderungen 26.08.2022

Drei-Säulen-Konzept, Standortunabhängigkeit, Datenrekonstruktion – die Experten brachten beim Roundtable IT-Security vielfältige Perspektiven ein. Warum ein gedrucktes Handbuch auch in digitalen Zeiten wichtig ist, und dass es bei Erpressung auch um Datenveröffentlichung gehen kann, berichtet Michaela Ortis.



Digitalisierung ist nicht nur ein Trend, sondern eine Notwendigkeit, um wettbewerbsfähig zu bleiben. Zur Digitalisierung gehören jedoch auch Cyberbedrohungen und IT-Sicherheit ist daher ein Bereich, um den sich alle Unternehmen kümmern müssen. Die Security-Herausforderungen werden merkbar größer, egal welche IT-News man liest, immer ist mindestens eine Meldung über Cyberattacken dabei. So meldet etwa KPMG, dass im letzten Jahr 67 Prozent der österreichischen Unternehmen Opfer eines Cyberangriffs waren, für 20 Prozent entstand daraus ein finanzieller Schaden. Steigende Bedrohungen gehen von Ransomware Angriffen aus. Das große Aber: Nur jedes fünfte heimische Unternehmen hat einen Krisen- oder Notfallplan, sagt der Deloitte Cyber Security Report 2022. Angesichts dieser bedrohlichen Zahlen nutzten

die Experten den Round Table, um ihr praxisorientiertes Wissen über Gefahren und Schutzmaßnahmen weiterzugeben.

Foto: Tim Gouw
Die Vielzahl an Cyber-Bedrohungen, denen Unternehmen ausgesetzt sind, erfordern eine ebenso große Zahl an Maßnahmen, die laufend evaluiert werden müssen
(/public/uploads/article/3554/pexels-tim-gouw-52608_klein.jpg)

Professionelle Attacken langfristig vorbereitet

„Wenn wir mit unseren Kunden sprechen und uns Trends ansehen, dann steht ganz oben auf der Liste das Thema Ransomware: Ein Unternehmen wird angegriffen und seine Daten verschlüsselt, um Geld erpressen zu können, damit es die Daten wieder entschlüsselt zurückbekommt. Die zweite große Bedrohung sind DDoS Attacken, durch die eine Vielzahl von Anfragen auf öffentlich verfügbare Dienste eines Unternehmens erfolgen, sodass dieses nicht mehr in der Lage ist, nach außen zu kommunizieren“, beschrieb Peter Bauer, IT-Security Spezialist im Account Management bei Bacher Systems, die aktuelle Cybergefahrenlage. Aus seiner Sicht habe sich mittlerweile die Hackerszene professionalisiert. Er beobachte einen Wandel weg von zufälligen Angriffen, wo eine große Masse an Unternehmen automatisiert nach leichten Zielen abgescannt werden. Stattdessen gebe es mehr gezielte Angriffe, so Bauer weiter: „Über lange Zeit werden große Unternehmen oder Organisationen ausspioniert und Informationen eingeholt, um dort gezielt einen Angriff zu setzen. Möglicherweise erfolgt ein strategischer Scheinangriff oder ein Ablenkungsmanöver. Mit kleinen Schritten versuchen Hacker irgendwo einzudringen, sich einzunisten und dann warten sie, ob das aufgefallen ist. Das kann Monate dauern und ist vergleichbar mit einem Schläfer in der physischen Welt, der irgendwo eingeschleust wird und auf sein Kommando wartet, um aktiv zu werden. Dasselbe passiert auch in der digitalen Welt. Da wir bei Bacher Systems auch beim Aufräumen nach einem Angriff unterstützen, zeigt sich in der forensischen Analyse, dass die eigentliche Ursache des Angriffs oft viele Monate zurückliegt.“

Das große Ganze im Auge haben

Foto: Georg Wilke

Dass Attacken in vielen Schritten erfolgen, bestätigte Stefan Schachinger, Produktmanager im Network Security Team von Barracuda Networks und er betonte daher, dass Bedrohungsszenarien nicht isoliert, sondern verknüpft betrachtet werden müssen: „Phishing ist immer schon ein Thema und meist der Beginn von etwas Größerem. Es kann der Anfang einer Ransomware-Attacke sein, da kommt ein Mail, jemand klickt darauf und es nimmt seinen Lauf. Ransomware ist der Worst Case für Unternehmen, verbunden mit

Zahlungen oder einem längeren Ausfall, den sie vermeiden möchten. Wir stellen in unserer Arbeit die Frage: Was muss passieren, damit eine Firma Lösegeld in Millionenhöhe zahlt. Da ist ein einziges Mail oder ein verschlüsselter Laptop nicht genug, sondern es braucht eine Reihe erfolgreicher Attacken, auch im internen Netzwerk, um das Unternehmen so zu schädigen, dass es zahlt. Man muss daher das große Ganze im Auge haben." Auf die Frage, wer besonders bedroht sei, zitierte er aus der Studie ´The State of Industrial Security in 2022´ von Barracuda Networks: Von den 800 befragten Unternehmen aus Industrie und kritischer Infrastruktur hatten 94% irgendeine Art von Sicherheitsvorfall, größere Unternehmen seien stärker betroffen. Schachinger überlegte dabei, wie sich das weiterentwickeln könnte: „Die großen Firmen implementieren auch mehr Security. Wenn sie also besser werden, verschiebt sich der Fokus der Angreifer Richtung Mittelstand? Auch eine kleine Steuerberatungskanzlei mit vier oder fünf Mitarbeitern hat mir schon von einem Vorfall berichtet. Wir stellen fest, dass die Angreifer ihre Hausaufgaben machen: Sie passen die Lösegeldforderungen an das Niveau des Unternehmens an, sodass es sich auch leisten kann zu zahlen."

Peter Bauer, Bacher Systems: „Die eine Schutzmaßnahme gegen Cyberangriffe gibt es nicht. Es ist immer eine Kombination einer Vielzahl von Maßnahmen, bezogen auf Menschen, Prozesse und Technologien."

(/public/uploads/article/3554/Peter Bauer__Credit Georg Wilke _klein.jpg)

Merkbarer Wandel bei Ransomware-Angriffen

Zu Markus Häfele, Geschäftsführer bei Attingo Datenrettung, kommen die Unternehmen, wenn bereits ein Angriff passiert und ihre Daten verschlüsselt sind und er meinte sinngemäß: „Wir sind die Feuerwehr." Auch Häfele hat schon strategische längere Angriffe beobachtet: „Es gab einige Fälle, wo wir im Nachhinein analysiert haben, dass beispielsweise Dateisystemtreiber manipuliert worden waren, damit auch die Backups schon verschlüsselte Daten enthalten. Das ist ein perfider Angriff mit Zeitfaktor, weil mehrere Generationen von Backups auf diese Weise verschlüsselt und somit vernichtet werden." Wenn mittels Ransomware Produktivdaten verschlüsselt wurden, könne Attingo ja nach Angriffsszenario helfen: Manchmal sei die Verschlüsselung nicht ganz vollständig durchgeführt, dann könnten die wertvollen Daten rekonstruiert werden, das komme aber immer

Foto: privat

Stefan Schachinger, Barracuda Networks: „Wir müssen weg von der Firewall im Rechenzentrum, wo alles darüber gehen muss. Mit Cloud und Home-Office müssen wir Security standortunabhängig implementieren."

(/public/uploads/article

/3554/Stefan Schachinger _ privat_klein.jpg)

seltener vor. Besser stehen die Chancen, wenn Backups durch die Angreifer unprofessionell vernichtet bzw. gelöscht worden sind. Es gab auch schon Fälle, wo ein Backup-Server zwei Tage vorher durch einen Festplattenausfall zum Stillstand gekommen war, dadurch kein Angriff mehr möglich und somit eine Datenrettung erfolgreich war. Definitiv sei ein Wandel in den Cyberangriffen merkbar, denn vor etwa fünf Jahren hätten Cyberkriminelle mit dem Gießkannenprinzip begonnen, dann folgten gezieltere Angriffe etwa über Exchange Server Lücken und nun gehe es zunehmend in Richtung größerer Unternehmen mit noch erweiterten Erpressungsversuchen, berichtete Häfele: „Nicht nur mit Verschlüsselung wird erpresst, sondern auch mit Veröffentlichung der Daten, die abgesaugt wurden. Das ist für Hacker noch vielversprechender, denn selbst wenn es ein Backup gibt und ein angegriffenes Unternehmen wieder produktiv arbeiten kann, wird es trotzdem zahlen, weil es die Veröffentlichung der Daten verhindern will."

Maßnahmen zum Schutz gegen Cyberbedrohungen

Beim Thema Daten veröffentlichen hakte Peter Bauer ein: „Es geht nicht nur um die Veröffentlichung der eigenen Unternehmensdaten, sondern da steht die Drohung im Raum, dass auch Daten von Kunden oder Geschäftspartnern durch Cyberkriminelle öffentlich gemacht werden und das ist besonders unangenehm." Auf die Frage, wie Unternehmen sich dagegen schützen können, betonte Bauer zwei Punkte: „Erstens müssen Cybersecurity-Maßnahmen Chefsache sein: Aus meiner Sicht ist das kein Thema der IT-Abteilung, die kann Technologien liefern, es braucht jedoch den Rückhalt des Managements. Zweitens muss Security im Unternehmen von den drei Säulen Menschen, Prozesse und Technologie gemeinsam getragen werden." Bei den Menschen ginge es um die Awareness der IT-Nutzer und diese werde besser, je mehr darüber berichtet wird, auch dieser Round Table trage dazu bei. Prozesse bedeute, dass Security keine einmalige Maßnahme sei, sondern ein fortwährender Anpassungsprozess. Technologie stehe meist im Vordergrund, aber funktioniere nur mit den beiden anderen Säulen.

Foto: Attingo
Wenn trotz vieler Schutzmaßnahmen ein Angriff erfolgreich ist, raten Datenretter Betroffenen vor allem, einen kühlen Kopf zu bewahren

(/public/uploads/article/3554/Attingo Datenrettung - Cleanroom Engineer_klein.jpg)

Awareness war auch für Stefan Schachinger ein wichtiges Thema, obwohl hundert Prozent nie

erreichbar seien. Die Bedeutung von Prozessen und Dokumentation unterstrich er mit Vorfällen aus der Vergangenheit: „Kriminelle timen ihre Angriffe und legen sie auf lange Wochenenden oder Feiertage. So sind beispielsweise Foxconn und Randstad am Thanksgiving-Day angegriffen worden. Daher muss geklärt sein, was zu passieren hat, wenn kaum jemand in der Firma ist." Als Hersteller von Sicherheitslösungen lege Barracuda Networks den Fokus auf Technologie, die dritte genannte Säule und da habe sich in den letzten Jahren viel bei Arbeitsweisen und Infrastruktur geändert: Denn Mitarbeiter arbeiten vermehrt im Home-Office und Unternehmen setzen verstärkt auf Cloudservices. Das Konzept der Perimeter Sicherheit, realisiert durch eine Firewall zwischen Unternehmensnetz und dem öffentlichen Internet, greife nicht mehr, folgerte Schachinger: „Bereits 2014 haben wir die Perimeter Security auf einer Konferenz für tot erklärt, aber die Pandemie hat gezeigt, dass sie immer noch vorhanden war. Jetzt sollten Unternehmen ihr Konzept überdenken und Security beim Benutzer oder am Endgerät implementieren. Es kann nicht sein, dass ich im Büro Sicherheitsmaßnahmen habe, die beispielsweise im Hintergrund, ohne die Nutzer zu stören, bösartigen Webtraffic ausfiltern, aber im Home-Office gibt es das nicht. Auch im Netzwerk zu Hause kann man Schadsoftware haben. Unternehmen müssen ein einheitliches Sicherheitsniveau unabhängig vom Standort schaffen und da sind neue Konzepte gefragt wie Zero-Trust, das ein Riesenthema ist." Ein Heimnetzwerk sei nicht vertrauenswürdig, genauso wenig ein WLAN am Flughafen oder in der Bahn, wo unbekannte Teilnehmer dabei sind. Sicherheitsmaßnahmen müssten daher an das Device gebunden werden und Unternehmen müssten weg vom Data Center Ansatz kommen. „Das Motto: Ich baue mir eine hohe Mauer und lasse nichts herein, funktioniert nicht mehr. Das sehen wir bei den heutigen Angriffsstrategien, denn eine Ransomware Attacke passiert nicht, indem was hereinkommt, jemand klickt drauf und zehn Sekunden später geht die Welt unter. Sondern wir müssen in der Lage sein, einen Angriff, der am Laufen ist, noch zu stoppen", führte Schachinger aus.

Was tun im Schadensfall

Trotz vieler Schutzmaßnahmen kann ein Angriff passieren und Markus Häfele erläuterte, wie man sich dann verhalten soll: „Der wichtigste Rat lautet: Kühlen Kopf bewahren und möglichst wenig in der Aufregung selber machen, sondern sich Unterstützung holen. Wir haben schon Fälle erlebt, wo das Produktivsystem mit den ursprünglichen Datenträgern neu aufgesetzt und somit überschrieben wurde. Da nimmt man sich jede Chance für Analyse und Rekonstruktion etwaig rettbarer Daten. Der Schritt davor wäre Security by Design. Das heißt, es müssen nicht alle Systeme wie NAS, Smarthome/IoT oder Web-Applikationen am externen Netz hängen und für alle per TCP/IP abrufbar

Foto: Patrick Kalteis
Markus Häfele, Attingo Datenrettung: „Gezielte Angriffe finden häufig auch

sein. Für das Backup ist empfehlenswert, dass es ein Offlinemedium gibt, weil alles, was nicht mit dem System verbunden ist, kann durch einen Angreifer auch nicht zerstört werden." Das könne, je nach Konstellation der Systeme, ein Band oder eine externe Festplatte sein. Wer mehrere Generationen von Backups aufbewahrt, sei noch einen Schritt mehr auf der sicheren Seite. Wie Attingo beim Rekonstruieren von Daten vorgeht, erläuterte Häfele ebenfalls: „Zuerst erstellen wir mehrere 1:1 Clones, um mit diesen Arbeitskopien parallel arbeiten zu können. Dann startet die Suche nach der Nadel im Heuhaufen: Welche Rohdaten sind noch vorhanden, sind Daten vollständig, gibt es kürzlich gelöschte Daten auf die man noch zugreifen kann. Es gibt kein Kochrezept, sondern immer verschiedene individuelle Szenarien." In einem Fall wurde etwa ein Kunde an sechs Standorten europaweit angegriffen und auf jedem Server seien die Hacker unterschiedlich vorgegangen; teils seien die Daten verloren gewesen, teils konnten sie rekonstruiert werden. Der Erfolg sei abhängig von der Systemarchitektur und dem Know-how der Angreifer und da gäbe es große Unterschiede.

am Wochenende statt, wenn weniger Mitarbeiter anwesend sind, die das erkennen können. Angreifer haben so ein paar Stunden mehr Zeit."

(/public/uploads/article/3554/Markus Haefele _ Credit Patrick Kaltseis_klein.jpg)

Damit Mitarbeiter bei einem Angriff richtig reagieren, müsse man schon vorher Schritte setzen, antwortete Bauer und nannte dazu die Abkürzung BCM: „Der Plan, der beschreibt was ich tun soll, wenn etwas passiert, ist Teil von Business Continuity Management. Erstes Gebot ist Ruhe bewahren. Der zweite Schritt ist, das Notfallhandbuch in die Hand zu nehmen, das hoffentlich nicht elektronisch abgelegt ist, wo ich nicht mehr zugreifen kann, sondern das klassisch als physischer Ordner im Regal steht." Dieser Plan brauche Planung und diese wiederum brauche genügend Analysezeit. Das Notfallhandbuch müsse beispielsweise Anleitungen erhalten, was zu tun ist, wenn Daten verschlüsselt sind, bzw. wie und worauf Daten wiederhergestellt werden. So wie sich die IT weiterentwickle, müsse auch der BCM-Plan ständig weiterentwickelt werden. Nicht vergessen dürfe man auf Notfallübungen, betonte Bauer: „Ich muss testen, ob das, was ich mir überlegt habe, in der Praxis auch funktioniert. Wir machen das für unsere Kunden, indem wir uns Szenarien überlegen und Teile davon mehrmals pro Jahr durchspielen."

Security ist nie fertig

Viele Bedrohungen erfordern eine Vielzahl an Maßnahmen, die laufend evaluiert und angepasst werden müssen, waren sich die Experten einig. „Wir haben es mit gut vorbereiteten Attacken zu tun. Der einzige Schutz ist Defense-in-Depth mit mehreren hintereinander gelagerten Schichten. Jede einzelne Schicht sollte den Angriff abwehren können, aber es ist die Kombination, die es ausmacht, dass ein Angreifer nicht eindringen kann oder gestoppt wird. Vor allem bei Cloud Services und IoT wird noch wenig getan. Mein Rat ist, klein anzufangen und Security als kontinuierlichen Prozess zu leben", empfahl Schachinger abschließend. Wie

Unternehmen vorgehen sollen, fasste Bauer zusammen: „Wir raten zu einer Bestandsaufnahme, um Handlungsfelder zu identifizieren. Davon werden Maßnahmen bezüglich Menschen, Prozesse und Technologie abgeleitet und es wird ersichtlich, mit welchem Aufwand ich wieviel mehr Schutz erreichen kann. Das kann ein klassischer Basisschutz sein, wie Perimeter- und Endpoint-Security und jede Art von Zugriff zumindest über Multifaktor-Authentifizierung abzusichern Der erweiterte Schutz ist die höhere Spielklasse, um etwa privilegierte Zugriffe auf Komponenten der IT-Infrastruktur nur noch nachvollziehbar und über einen Session Manager zu erlauben. Oder Analysemethoden für Aktivitäten im Netz einzusetzen und technologie-unterstützte Policies für die Nutzung von Cloud Assets zu erstellen. Markus Häfele war es wichtig, nochmals auf das Thema Awareness hinzuweisen: „Es gibt auch Fälle, wo Angreifer einzelne Mitarbeiter bestochen haben; man sollte nicht außer Acht lassen, dass manche kompromittierbar sind. Beim Ausarbeiten des Notfallkonzepts sollten sich Unternehmen außerdem Gedanken machen, ob sie auch die benötigte Infrastruktur haben, um das System wieder ins Laufen zu bringen."

Die Sprecher beim Security Round Table

- ***Peter Bauer*** *ist IT-Security-Spezialist im Account Management bei Bacher Systems und berät Kunden bei Planung und Umsetzung von IT-Security Vorhaben. Schwerpunkt liegt unter anderem auf Lösungen, die Cyber-Kriminalität durch das Ausnützen von privilegierten Benutzerkonten verhindern.*
- ***Markus Häfele*** *ist bei Attingo Datenrettung seit anderthalb Jahren Mitglied der Geschäftsleitung. Zuständig für das Tagesgeschäft kommuniziert er viel mit den Kunden und fungiert gleichsam als Übersetzer für die Techniker-Welt.*
- ***Stefan Schachinger*** *vertritt als Produktmanager im Network Security Team beim internationalen Anbieter Barracuda Networks die Produktentwicklung. Dabei unterstützt er Kunden und Partner bei der Konzeption von Sicherheitslösungen.*

Den Talk zum Nachsehen finden Sie auf unserem YouTube-Kanal (https://www.youtube.com/channel/UCNVYRW3sxmozr9C1bHFs0CA).

#SECURITY (/artikel/security)

---

office@ittbusiness.at (mailto:office@ittbusiness.at)

IMPRESSUM (/IMPRESSUM)

DATENSCHUTZ (/DATENSCHUTZ)

WEBSITE BY NIKOLL.AT (HTTP://WWW.NIKOLL.AT/)