LICENSEE OF IDG COMMUNICATIONS
www.computerwelt.at
20.03.2019 | EUR 3,

COMPUTERWELT

MÄRZ 2019

HERAUSFORDERUNG MULTICLOUD

Im Zuge der zunehmenden Nutzung verschiedener Cloud-Services wird das Management über mehrere Clouds hinweg zur Königsdisziplin.

»CYBERSECURITY-AWARENESS IST DA«

Das IT-Security-Geschäft »brummt«. Der Amstettner Security-Dienstleister Antares-Netlogix profitiert davon enorm und ist auf Expansionskurs. Gründer Alexander Graf spricht im COMPUTERWELT-Interview über aktuelle Security-Herausforderungen.

Wo liegen derzeit in der Arbeit mit Ihren Unternehmenskunden die Schwerpunkte?
Wir haben aktuell rund 300 Kunden in ganz Österreich und adressieren mittelständische und große Kunden ab circa 100 IT-Arbeitsplätzen, wie etwa ÖAMTC oder Städte, viele Hidden Champions aus der Industrie, Energieversorger oder die Vorarlberger Landesversicherung. Derzeit sehen wir drei Schwerpunkte: erstens setzen wir auf Infrastruktur-Optimierung, das heißt die Verfügbarkeit möglichst hoch zu halten, ob kabelgebunden oder wireless. Wir unterstützen zweitens die Kunden weltweit bei der Absicherung ihrer Standorte und Rechenzentren, wie zum Beispiel Tyrolit. Wir sind auch verantwortlich für die Sicherheit des österreichischen Bankomat-Rechenzentrums der payment Service Austria. Dritter Schwerpunkt ist die Betriebsübernahme und -unterstützung, das heißt wir betreiben die Rechenzentren oder Netzwerk-Umgebung für die Kunden als Managed Service. Da betreuen wir inzwischen fast schon 600 Server und haben ein 7x24-Team, es sind also immer drei Kollegen in Bereitschaft. Wir haben zudem in Wien ein redundantes Rechenzentrum und sind selbst auch Internet Provider. Nach Netzwerk-Sicherheit ist auch das Thema Access – das heißt wer darf in mein Netzwerk und wer nicht – sehr gefragt. In letzter Zeit ist außerdem Verschlüsselung ein großes Thema, vor allem im Mailverkehr.

Das heißt die IT-Security-Awareness und Bereitschaft, dafür Geld zu investieren, ist inzwischen da oder ist es immer noch ein Thema, das man gern zur Seite schiebt?
Ich denke, alle größeren Unternehmen haben erkannt, dass IT-Security ein wichtiges Thema ist. Aufgrund extrem vieler Vorfälle in den


Alexander Graf ist Gründer und CTO von Antares-NetlogiX.

letzten zwei, drei Jahren ist die Awareness groß. Auch im Vorstand ist die Cybersecurity Awareness jetzt da, es wird bei der IT nachgefragt: Wie sicher sind wir? Wir bewegen uns außerdem bei Schadenssummen im sechsstelligen Euro-Bereich, das schafft entsprechende Awareness.

Es geht ja auch um Schutz vor Stillstand oder Produktionsausfällen, das heißt wie sollte ein vorausschauendes Business Continuity Management (BCM) aussehen?
Der erste Schritt ist immer die Awareness. Krisenvorsorge ist ein negativ besetztes Thema, dabei sind die Gefahren heute um einiges vielfältiger und komplexer als noch vor zehn Jahren. Meist sind Erlebnisse wie eine Naturkatastrophe, ein Cyberangriff oder ein simpler Stromausfall der Auslöser für die ersten Schritte. Oder Standards und Rechtsvorschriften müssen umgesetzt werden. Ein konkretes Projekt beginnt meist mit einem Notfallhandbuch und einer Unternehmensanalyse bis hin zum Einsatz einer BCM-Software inklusive Monitoring und Alarmierung der Belegschaft via Smartphone. Der technisch viel spannendere Teil ist das Disaster Testing. Dabei wird das IT-System stromlos gemacht oder geplant heruntergefahren und ebenso wieder hochgefahren. Hier haben wir eine Lösung entwickelt, die es so am Markt noch nicht gibt: Wir können damit Hardware, Software und die virtuelle Cloud-Welt mit individuellen Logiken managen – also viel mehr als eine klassische USV-Software.

Nächstes Thema: Die zunehmende Vernetzung, Stichwort IoT, ist eine große Herausforderung in punkto IT-Security. Wie können sich Unternehmen hier schützen?
Wir sehen in den letzten Jahren, dass im Bereich IT-Infrastruktur und Security mehrere Themen gleichzeitig angegangen werden müssen. Gerade die technischen Anforderungen aus der Produktion durch zum Beispiel Netzwerksegmentierung, aber auch die an Webportale durch Web-Application-Firewalls, sind hoch.
Wichtig sind auch kleinere, relativ simple Maßnahmen: Administratoren sollten zum Beispiel das Passwort-Management im Auge behalten, das empfiehlt sich auch aus Datenschutzgründen. Hier spielen zudem Themen wie die PKI-Frage (Public Key Infrastruktur) und die Zwei-Faktor-Authentifizierung eine Rolle, wofür wir ebenfalls Lösungen anbieten. Gerade E-Mail-Verschlüsselung und sicherer verschlüsselter Mail-Transport ist für viele Unternehmen ein Thema, das jetzt umgesetzt wird.

»Das Problem ist, dass IT-Security-Fachkräfte im Moment nur sehr schwer zu bekommen sind.«

Speziell in der IoT-Welt kommen Sie ohne Penetration-Tests und Log-Management nicht weit, hier setzen wir auf eigenes Knowhow und eigene Software. Ebenso ist es wichtig, Patches und Schwachstellen-Scans monatlich durchzuführen, wodurch Managed Security Services eigentlich unumgänglich sind, wenn nicht ein eigenes Security Operations Center (SOC) betrieben wird.
Wir sehen in dem Bereich auch eine wirklich große Nachfrage. Daher sind wir gerade dabei, unser eigenes SOC zu vergrößern und suchen dafür Mitarbeiter. Das Problem ist, dass IT-Security-Fachkräfte im Moment nur sehr schwer zu bekommen sind. Die Ausbildung an den HTLs in St. Pölten und Ybbs, an den FHs und Unis ist zwar gut, aber der Nachwuchs wird schon während der Ausbildung vom Fleck weg engagiert.

Welche Gefahren lauern denn, welche Angriffsarten kommen hauptsächlich vor, um Unternehmen zu schädigen?
Phishing-Attacken und etwa CEO-Frauds sind heute sehr beliebt, um Mitarbeiter irrezuführen. Die Angreifer recherchieren inzwischen sehr gut über die Firmen, die Angriffe sind viel professioneller und gezielter geworden. Sehr oft sehen wir in letzter Zeit Verschlüsselungsangriffe. Ich war erst unlängst bei einem Interessenten, der war vier Tage lang handlungsunfähig. Das kann in manchen Branchen schon ein Riesenproblem sein.

Woran hapert es denn bei den Mitarbeitern in den Unternehmen in punkto IT-Security?
Der Erfolg von Fake-Mails und CEO-Frauds liegt vor allem daran, dass es bei der Kommunikation hapert. Je besser die Mitarbeiter im Unternehmen kommunizieren, je besser die Unternehmenskultur und der Umgang miteinander, desto geringer ist die Chance, dass ein Angriff funktioniert. Natürlich muss auch eine Schulung der Mitarbeiter erfolgen, und die muss wiederkehrend sein. Wichtig ist: Es muss für alle verständlich und vom Umfang her überschaubar sein. Es gibt dafür schöne Schulungsplattformen.

Und technologisch, was empfehlen Sie, um eine moderne IT-Sicherheitsarchitektur aufzubauen?
Weil die Angriffe immer intelligenter werden, muss auch die IT-Security immer intelligenter aufgebaut werden. Es gibt viele Einfalls-Szenarien, aber die E-Mail birgt über Phishing oder Trojaner immer noch das größte Gefahrenpotenzial.
Hier helfen sogenannte Sandboxing-Systeme, die im Vorfeld simulieren, ob etwas Böses passiert, wenn etwa ein Link angeklickt wird.
Stichwort Mobility: Alle mobilen Endgeräte sollten verschlüsselt sein. Eine weitere Maßnahme ist es, die Schnittstellen der Endgeräte abzusichern, damit sich nicht jeder Mitarbeiter via USB-Stick etwas einfangen kann. Wir brauchen also eine Endpoint Security mit erweiterter Sicht.

| CHRISTINE WAHLMÜLLER

Am 8. Mai 2019 erscheint in der COMPUTERWELT die Magazinbeilage

Anzeigen- und Redaktionsschluss: 19. April 2019

IHRE ANSPRECHPARTNER IN DER ANZEIGENABTEILUNG:

Martina Jedlicka
martina.jedlicka@cwverlag.at
+43 699 | 104 04 228

Sabine Pachler
sabine.pachler@cwverlag.at
+43 660 | 876 63 95

IHRE ANSPRECHPARTNER IN DER REDAKTION:

Oliver Weiss
oliver.weiss@cwverlag.at

Alexander Wolschann
alexander.wolschann@cwverlag.at