Interview

Einen angemessenen Schutz aufbauen

Alexander Starke über effektive Maßnahmen, IT-Notfallpläne und das Ende des sicheren Hafens.

Wie sind Ihre Erfahrungen als Dienstleister: Wappnen sich kleine und mittlere Unternehmen (KMU) ausreichend vor Cybercrime?
Wie wir am Markt beobachten, schützen sich KMU häufig nicht ausreichend vor Cybercrime. Allerdings hat das Schutzlevel in jüngerer Vergangenheit deutlich zugenommen. Das liegt unter anderem daran, dass es mehr bekannte Fälle im direkten Umfeld gibt. Wichtig ist: Wir müssen über solche Fälle und Abwehrmöglichkeiten reden – sonst überlassen wir Cyberkriminellen das Feld. Im besten Fall ersparen Betroffene dadurch anderen Unternehmen und Organisationen, was sie selbst durchmachen mussten. Klar ist dabei zugleich auch: Einen 100-prozentigen Schutz gibt es nicht – schon gar nicht auf eine für jede Firma wirtschaftlich sinnvolle Weise. Entscheidend ist am Ende, dass jedes Unternehmen ein angemessenes individuelles Schutzniveau aufbaut und pflegt – abhängig davon, wie intensiv es IT nutzt beziehungsweise wie stark es auf sie angewiesen ist.

Die Zahl erfasster Cyber-Straftaten hat laut Polizeilicher Kriminalstatistik im vergangenen Jahr einen neuen Höchstwert erreicht. Dennoch verfügen circa 60 Prozent der Unternehmen bundesweit nicht über einen IT-Notfallplan, wie eine DIHK-Umfrage ergeben hat. Warum zahlt es sich aus, in einen solchen zu investieren?
Infolge der stärkeren Digitalisierung müssen sich KMU auf ihre IT und die Sicherheit selbiger verlassen können. Notfallpläne bilden dafür eine wichtige Grundlage: Wen spreche ich im Ernstfall zuerst an, wer ist der Vertreter? Wen brauche ich wofür? Muss ich vielleicht zuerst meine Cyberversicherung anrufen, bevor ich tätig werde? Falsche Ad-hoc-Maßnahmen können die Lage sogar verschlimmern. Notfallpläne reichen bis hin zu Konzepten und Wiederanlaufplänen, um schnellstmöglich wieder arbeitsfähig zu werden. Das Schöne an ihnen ist: Am Ende stellen sie ein Extrakt aus sehr vielen Basisinformationen dar, die man für den Regelbetrieb oder für das Design der IT-Architektur ohnehin benötigt. Um solche Pläne sinnvoll aufzubauen, müssen sich Unternehmen zuvor damit beschäftigt haben, welche konkreten Auswirkungen ein Ausfall bestimmter Systeme auf den Betriebsalltag und ihr Geschäftsmodell haben. Daraus lassen sich verschiedene Maßnahmen und Schritte ableiten. Informationen und Unterstützung bieten auch die IHK Kassel-Marburg und das IT-Netzwerk Nordhessen, zum Beispiel mit kostenfreien Veranstaltungen wie dem IT-Security-Day am 5. Oktober.

> „Falsche Ad-hoc-Maßnahmen können die Lage sogar verschlimmern.

60

Prozent der Unternehmen bundesweit haben keinen IT-Notfallplan, wie eine Umfrage des Deutschen Industrie- und Handelskammertags (DIHK) ergeben hat.

Was hindert Mittelständler aus Ihrer Sicht daran, Ressourcen in eine belastbarere IT-Sicherheitsinfrastruktur zu stecken?
Die Gründe sind relativ vielschichtig. Nach dem einmaligen Kauf eines Virenschutzes oder einer Firewall-Lösung verlassen sich zu viele noch darauf, für lange Zeit geschützt zu sein – eine falsche Vorstellung. Elementar ist, sich regelmäßig um IT-Sicherheit zu kümmern und sie zu pflegen. Die Angreifer suchen das schwächste Glied in der Kette. Wenn sie beispielsweise über das offene Firmen-WLAN vom Parkplatz in ihre Systeme gelangen, hilft selbst die sicherste Firewall nicht weiter. Daran wird deutlich: Ganzheitliches Denken und der Blick auf die komplette Umgebung sind wesentlich, das Geschäftsmodell spielt eine weitere Rolle. Zudem schreckt einige ab, dass IT-Sicherheit erstmal viel Geld kosten könnte. Ich glaube aber nicht, dass das immer der Fall sein muss.

Haben Sie Beispiele für günstige Lösungen?
Ein klassisches Beispiel ist die Überlegung, ob eine Firma einen eigenen Fileserver betreibt mit eigenen Dateien, die es zu sichern gilt, oder alternativ eine Cloud-Lösung nutzt, die bereits Speicher-

platz beinhaltet und eine sehr hohe Sicherheit garantiert. Für mich gibt es kaum Gründe, Cloud-Lösungen nicht zu nutzen. Wenn ich selbst als Unternehmen die Daten in einem Serverraum verwalte, ist das Sicherheitsniveau eklatant niedriger als das, was die kleinste Cloud-Lizenz ermöglicht. Diese Option sollte also nicht aus falschen Gründen abgelehnt werden. Trotzdem lohnt es nicht für jedes Unternehmen, in die Cloud zu gehen. Dreh- und Angelpunkt ist, sich zu überlegen, was das Unternehmen will und wo Sicherheitsrisiken bestehen.

Welche Schritte sollten KMU gehen, um ihre IT-Sicherheit zu erhöhen?
Zunächst sollten sie den Bestand vorhandener Sicherheitswerkzeuge wie Virenscanner, Firewall, Verschlüsselung, Archivierung und ähnliche Dinge ermitteln. Ist alles vorhanden und auf dem aktuellen Stand, bedarf es einer regelmäßigen Pflege. Darauf aufsetzend, ist es extrem wichtig, Daten regelmäßig zu sichern. Das muss so geschehen, dass auch diese vor Angriffen geschützt sind. Denn Trojaner verschlüsseln gern die Datensicherung mit. Planen Unternehmen neue IT-Lösungen einzuführen oder etwas an ihr zu ändern, sollten sie bereits im Vorfeld IT-Sicherheitsfragen mitdenken – so lässt sich in vielen Fällen ein höheres Sicherheitsniveau erreichen, ohne gleich exorbitant mehr bezahlen zu müssen. Insgesamt gilt: Die Hürden für Angreifer so hoch wie möglich hängen – und so hoch wie nötig. Denn wenn ich Daten so weit wegschließe, dass sie kein Anwender mehr nutzen kann, bringen sie auch nichts.

Eine resiliente IT-Infrastruktur ist das eine. Oft dient allerdings der Mensch als Einfallstor für Cyberkriminelle. Wie können KMU Vorsorge treffen, dass ihre Mitarbeiterinnen und Mitarbeiter nicht ungewollt als Türöffner fungieren?
Indem KMU sie im Umgang mit der IT und typischen Angriffsszenarien schulen und sensibilisieren. Woran lässt sich eine gefälschte Website erkennen? Wie läuft eine CEO-Fraud genannte Erpressung ab? Sehr hilfreich ist es, intern offen über Vorfälle und Auffälligkeiten aus dem Alltag zu sprechen. Viele Unternehmen sind bereits angegriffen worden, das weiß nur kaum jemand.

Wir müssen lernen, mit der Bedrohungslage umzugehen – sie wird nicht mehr verschwinden. Dazu gehört, nicht mehr darauf zu vertrauen, dass das interne Netzwerk einen sicheren Hafen darstellt. Wir müssen stets davon ausgehen, dass unsere IT-Infrastruktur betroffen, unsere IT-Umgebung von Späh- oder Schadsoftware befallen ist. Entsprechend sollte jeder Einzelne nur die Berechtigungen und Zugriffe haben, die reell benötigt werden – es ist nicht notwendig, jederman jederzeit mit Administrator-Rechten auszustatten.

FOTO: JÖRG LANTELMÉ

Zur Person

Alexander Starke führt seit 2014 mit seinem Cousin Felix Reichert die Geschäfte bei Starke+Reichert, einem IT-Systemhaus, Softwarehersteller und Büropartner mit Sitz in Kassel. Nach dem Abitur am Beruflichen Gymnasium May-Eyth-Schule mit Schwerpunkt Datenverarbeitungstechnik studierte Starke Wirtschaftsinformatik in Fulda. Danach war er für eine Beratungsfirma in der IT-Prozessberatung in Konzernen unterwegs, bevor er 2012 in das Familienunternehmen eingestiegen ist. Ehrenamtlich engagiert sich der 38-Jährige nicht nur in der IHK-Vollversammlung und als stellvertretender Vorsitzender des Handelsausschusses sowie des Ausschusses für Infrastruktur, Verkehr und Logistik, sondern auch im DIHK-Mittelstandsausschuss und bei den Wirtschaftsjunioren. Seine Freizeit verbringt er gern mit seiner Ehefrau und den zwei Kindern in der Natur.

> „Wenn ich Daten so weit wegschließe, dass sie kein Anwender mehr nutzen kann, bringen sie auch nichts.

Ist es überhaupt noch möglich, mit dem Entwickeln und Bereitstellen effektiver Schutzwerkzeuge hinterherzukommen?
Es ist kein Hinterherkommen, sondern ein Hinterherrennen – im Prinzip ein Wettrüsten zwischen Angreifern und Sicherheitsindustrie. Die Frage ist: Wer erkennt die Lücken und Risiken zuerst? Wer hat sie zuerst ausgenutzt oder gestopft? Mittlerweile hat die Sicherheitsindustrie Lösungen auf Basis neuer Technologien wie Cloud und Künstliche Intelligenz (KI) entwickelt, um Unregelmäßigkeiten und Auffälligkeiten zu erkennen und abzuwehren. Doch selbst wenn eine solche Lücke gestopft ist, muss diese Lösung immer noch direkt in den Unternehmen ankommen. Schon sind wir wieder bei der kontinuierlichen Pflege und regelmäßigen Updates – ohne diese profitieren Unternehmen natürlich nicht vom erweiterten Schutz.

Das Interview führte Andreas Nordlohne