«Jede Firma benötigt dringend einen ‹Plan B›»

Die Digitalisierung eröffnet Unternehmen aller Branchen und Grössen ungeahnte Chancen. Doch mit der zunehmenden Abhängigkeit von Online-Services und Automatisierung entstehen auch neue Gefahren: Die Anzahl der Hacker-Angriffe nehmen zu und sind für betroffene Unternehmen oft existenzbedrohend. Wir wollten von einem Experten wissen, welche Lösungsansätze es gibt.

Interview mit Urs Küderli, Partner, Leiter Cybersecurity und Privacy, PwC Schweiz

Urs Küderli

Urs Küderli, das Thema «Cybercrime» gewinnt immer mehr an Relevanz: Aktuelle Erhebungen, unter anderem zwei Studien von PwC, zeigen, dass die Gefährdung aus dem Netz zunimmt. Wie beurteilen Sie die Lage?
Es trifft in der Tat zu, dass die Anzahl der Angriffe ansteigt und auch die Art und Weise, wie diese erfolgen, immer facettenreicher und vor allem professioneller wird. Längst ist die Grösse eines Unternehmens nicht mehr als einziger Faktor ausschlaggebend dafür, ob man ein attraktives Ziel für Hacker:innen darstellt oder nicht. Auch ist das Gefährdungsrisiko eines Unternehmens nicht mehr nur abhängig von der Exposition: Banken gehörten lange zu den präferierten Opfern, da es dort potenziell Geld direkt zu holen gab, aber heute ist jedes Unternehmen im Fokus, so auch Industrie-, Retail- und KMU-Betriebe. Gerade auch Firmen im Pharmabereich sind anfällig, insbesondere für Spionage-Angriffe. Eine weitere Veränderung: Cybercrime ist heute deutlich «lauter» als früher. Bis vor Kurzem wurden Cyber-Angriffe von betroffenen Unternehmen teilweise gar nicht registriert und erst spät entdeckt. In den letzten zweieinhalb Jahren hat sich hier ein Wandel vollzogen. Sogenannte massive «Ransomware-Angriffe», bei denen Unternehmen durch die breite Verschlüsselung ihrer Systeme daran gehindert werden, ihrer Arbeit nachzukommen und damit erpresst werden, bestimmen das Bild. Zusätzlich werden vertrauliche Daten gestohlen, was die Firmen noch erpressbarer macht. Das sind Angriffe, die Firmen aufrütteln und Schlagzeilen generieren – auch weil sie hohe Schäden verursachen. Betroffene Firmen können durch derartige Attacken für Tage oder Wochen in die technologische Steinzeit zurückgeworfen werden. Etliche Betriebe kämpfen noch Jahre nach dem Angriff mit Folgen der Attacke.

Was geschieht in einem solchen Worst-Case?
Es sind sehr grundlegende Fragen, die in solchen Situationen schlagartig an Relevanz gewinnen: Wer ist verantwortlich für die weiteren Schritte? Wie sollen die Massnahmen aussehen, wie ermöglichen wir so schnell wie möglich einen Betrieb? Haben wir Backups, die nicht verschlüsselt wurden, wie spielen wir diese zurück? Im Falle von solchen massiven Ransomware-Angriffen werden ganze IT-Landschaften blockiert und dann ein Lösegeld per Bitcoin gefordert. Da stellt sich für viele Firmen die Frage, ob sie Lösegeld zahlen sollen – und wo sie eigentlich Bitcoin herbekommen. Der Stresspegel ist in einer solchen Extremsituation hoch, denn das Schadensspektrum reicht – je nach Fall – von 50 bis 150 Millionen Franken an direktem Schaden. Denn die betroffenen Firmen benötigen mindestens sieben bis zehn Tage, um in einen geordneten Betrieb zurückkehren zu können.

Wer sind die Angreifenden, die solche Cyber-Attacken verüben?
Das Spektrum reicht von Schüler:innen, die sich einen Spass daraus machen, eine Website lahmzulegen, bis hin zu staatlich geförderten Organisationen. Den Grossteil machen allerdings kriminelle Organisationen aus, für die Cybercrime zum Businessmodell geworden ist. Dabei handelt es sich überwiegend um kleine Unternehmen, die auf spezifische Aspekte von Cybercrime spezialisiert sind, wie Phishing, Social Engineering oder physische Attacken. Dadurch hat sich in diesem Feld eine regelrechte Ökonomie etabliert: Es gibt spezialisierte Gruppen, die in Firmen eindringen und diesen Zugriff dann weiterverkaufen – etwa an Kriminelle, die einer Organisation dann vertrauliche Firmen-Datensätze entwenden und diese weitervertreiben. Der Abnehmer bereitet die Daten anschliessend für die Übergabe an die nächsten Akteure auf, welche zum Schluss die Verschlüsselung sowie die Erpressung des geschädigten Unternehmens einleiten. Da gemäss aktuellen Erhebungen rund 70 Prozent der betroffenen Firmen das Lösegeld bezahlen, um ihre Systeme wieder entschlüsseln zu können, handelt es sich dabei um ein lukratives Business.

Stehen Unternehmen also auf verlorenem Posten angesichts der professionellen Angreifenden?
Es ist teilweise ein ungleicher Kampf, doch wer sich der Gefahren aus dem Netz bewusst ist, kann sich absichern. Genau dabei unterstützen wir vom Bereich Cybersecurity bei PwC Schweiz unsere Kundschaft. Wir fokussieren uns auf zwei essenzielle Aspekte: Zum einen geht es darum, Firmen auf mögliche Angriffe vorzubereiten und sie für den Ernstfall zu wappnen. Dafür konzentrieren wir uns stark auf das individuelle Bedrohungsszenario eines Unternehmens sowie auf dessen Möglichkeiten und Fähigkeiten. Wir helfen Firmen, sich auf den Krisenfall vorzubereiten, um schnellstmöglich reagieren und somit baldmöglichst den Betrieb wieder aufnehmen zu können. Zum anderen unterstützen wir unsere Kunden im Krisenmanagement in rechtlichen und technischen Aspekten, bei der Forensik, im Datenschutz sowie beim Wiederaufbau, sollte dieser Ernstfall eintreten. Die Summe dieser Massnahmen hilft Firmen dabei, resilienter gegen Angriffe zu werden – oder im Angriffsfall den Schaden zu minimieren.

Wie schätzen Sie die durchschnittliche digitale Resilienz von Schweizer Unternehmen ein?
Viele Betriebe haben ihre «Hausaufgaben» gemacht und sind heute deutlich besser geschützt, als dies noch vor einigen Jahren der Fall war. Doch die Angreifer:innen bleiben nicht stehen, sondern passen sich an: Oft ist es einfacher, einen kleinen Betrieb anzugreifen, der Teil der Lieferkette einer grösseren Unternehmung ist. Die meisten Firmen haben heute verschiedene Partner und Zulieferer, die nicht selten über privilegierten Zugriff auf Systeme und Daten verfügen. Das macht diese Firmen zu idealen Gateways für Kriminelle. Hinzu kommt, dass Produkte und Dienstleistungen, die von Dritten bezogen werden, ausserhalb der eigenen Kontrolle liegen. Um zu verhindern, dass sich Angreifer:innen über diese Partner Zugang zum eigenen System verschaffen, kann und sollte man nachfragen, welche Sicherheitsmassnahmen und -Zertifizierungen vorliegen. Zu viele Unternehmen haben wenig bis gar kein Verständnis für die IT und Software-Risiken in ihrer Lieferkette. Am Ursprung erfolgreicher Angriffe stehen aber noch immer oft Phishingmails und ungenügend gewartete Systeme.

Wo kann man ansetzen?
Grundsätzlich beginnt dies bei der Aufklärung und dem Schaffen von Verständnis, aber essenziell ist auch das Etablieren einer offenen Fehlerkultur. Wenn jemand in der Firma zum Beispiel eine Phishingmail öffnet und den Fehler bemerkt, kann es entscheidend sein, dass er oder sie den Fall sofort meldet. Dann kann man nämlich reagieren und den potenziellen Schaden eingrenzen. Ist eine solche Kultur nicht vorhanden, werden derartige Fehltritte vielleicht nicht oder erst spät kommuniziert – was den möglichen Folgeschaden erhöht.

Cybersecurity ist also ein komplexes Handlungsfeld, das sowohl technische Faktoren als auch Aspekte der Führung und Kommunikation umfasst. Wie läuft ein Mandat ab, wenn Unternehmen bei PwC diesbezüglich Unterstützung suchen?
Zuerst müssen wir natürlich unterscheiden, ob es sich beim Mandat um die Vorbereitung auf einen möglichen Angriff handelt oder ob dieser bereits geschehen ist. Ist Letzteres der Fall, begleiten wir die Kundschaft sehr eng durch den «Krisenmodus». Auf der technischen Ebene arbeiten wir dann zum Beispiel daran, sicherzustellen, dass nicht das gesamte System verschlüsselt wird. Ist es dafür bereits zu spät, fokussieren wir uns darauf, das Unternehmen so schnell wie möglich zurück zu einem funktionierenden System zu verhelfen. Das kann einen Neu- oder Teilneubau der IT-Umgebung voraussetzen. Gleichzeitig unterstützen wir das Management bei der Krisenorganisation und helfen auch bei der Kommunikation nach innen und aussen. Das oberste Ziel besteht immer darin, die Situation so schnell wie möglich wieder in den Griff zu bekommen. Einfacher – und deutlich weniger stressig – ist es, wenn wir proaktiv einbezogen werden, und nicht erst im Ernstfall.

Wo liegt dann der Fokus?
Wir erhöhen die Resilienz gezielt. Dazu führen wir unter anderem Assessments durch, um herauszufinden, wo das Unternehmen steht, etwa mit Krisensimulationen. Diese sind sehr nahe an realen Fällen angelegt und dienen der Erkennung von Schwachstellen. Gemeinsam mit dem Unternehmen erarbeiten unsere Fachleute dann Massnahmen, um diese blinden Flecken zu beheben. Ganz wichtig: Wir helfen unseren Kundinnen und Kunden dabei, einen «Plan B» auszuarbeiten. Wer nämlich im Ernstfall trotz Verschlüsselung von Daten und Systemen in der Lage ist, handlungsfähig zu bleiben, ist unweigerlich im Vorteil. Das kann etwa bedeuteten, alternative Systeme zu nutzen oder sogar eine gewisse Zeit lang auf Papier und Stift zurückzugreifen.

Wie wird sich Cybersecurity in Zukunft entwickeln?
Unsere Studien haben eine weitere Zunahme von Gefährdungen und Angriffen im virtuellen Raum gezeigt. Diese Tendenz bleibt ungebrochen, denn Cybercrime ist lukrativ und die Risiken sind vergleichsweise gering. Insgesamt hinken Unternehmen den kriminellen Organisationen hinterher. Aus diesem Grund muss es uns gelingen, möglichst viele Betriebe für das Thema «Cybersecurity» zu sensibilisieren und sie bei der Vorbereitung auf einen Angriff zu unterstützen.

Zum Schluss: Sollte man als Opfer eines Ransomware-Angriffs das Lösegeld zahlen, um den Schlüssel für die verschlüsselten Daten zu erhalten?
Wir empfehlen in der Regel, dies nicht zu tun. Diesen Entscheid muss letztlich jedes Unternehmen für sich fällen. Das Entrichten des Lösegelds ist längst kein Garant dafür, dass man einen funktionierenden Schlüssel erhält beziehungsweise die Daten in jedem Fall entschlüsselt werden können. Zudem muss man sich der rechtlichen Konsequenzen bewusst sein, etwa wenn man Geld an Akteure zahlt, die von sanktionierten Staaten aus operieren. Schlussendlich darf man nicht vergessen, dass man zwar in den meisten Fällen den Zugriff auf die Daten zurückerhält, aber die Umgebung ist noch immer infiziert, die Angreifer:innen im System und die Schwachstellen weiter vorhanden. Die Investition in die Reinigung der Umgebung, Beseitigung von Schwachstellen und mehr ist also trotzdem notwendig. Rechtzeitige Investitionen in einen guten «Plan B» sind auf jeden Fall die bessere Lösung.

Mehr Informationen zu den verschiedenen Cybersecurity-Lösungen von PwC Schweiz finden Sie hier:

Über PwC

PwC Schweiz ist das führende Prüfungs- und Beratungsunternehmen in der Schweiz. Der Zweck von PwC ist es, das Vertrauen in der Gesellschaft aufzubauen und wichtige Probleme zu lösen. Das Netzwerk von Firmen ist in 155 Ländern tätig und beschäftigt über 327000 Mitarbeitende. Diese setzen sich dafür ein, in den Bereichen Wirtschaftsprüfung, Beratung und Steuern erstklassige Dienstleistungen zu erbringen. PwC Schweiz hat über 3380 Mitarbeitende und Partner an 14 verschiedenen Standorten in der Schweiz sowie einem im Fürstentum Liechtenstein.