Acht Stufen meistern

Nachhaltige Cyber-Sicherheit

von Martin Andenmatten

Widerstandsfähigkeit wird zum kritischen Erfolgsfaktor, um Cyber-Attacken zu überleben. Der folgende Beitrag analysiert die Situation und gibt einige strategische Hinweise.

Man ist sich heute bewusst, dass mit der Nutzung von Cloud-Diensten nicht nur enorme Chancen offenbart werden, sondern darin auch grosse Risiken schlummern. Insbesondere die Sicherheit der Daten, welche in die Wolke verschoben wird, könnte kompromittiert werden und in falsche Hände gelangen. Verantwortungsbewusste Unternehmen wählen daher auch sehr gezielt die Datenbereiche aus, welche überhaupt mit Cloud-Diensten bearbeitet werden dürfen. Andere denken sich, dass niemand ernsthaft an ihren Daten interessiert sein kann und gehen diesbezüglich etwas sorgloser damit um. Dies gilt im geschäftlichen wie aber insbesondere auch im persönlichen Bereich. Eine Trennung in den Netzen ist heute kaum realisierbar, da alle mit ihren eigenen privaten mobilen Gerätschaften arbeiten

Was sich die wenigsten Unternehmen heute aber wirklich bewusst sind, ist die Tatsache, dass über ihre Firmennetze bereits mehrere hundert Cloud-Services genutzt werden, ohne dass die Verantwortlichen überhaupt Kentniss davon haben. Sie denken, niemals in ihrem Haus? Die Firma Skyhigh Networks (skyhighnetworks.com) ist auf das Aufspüren und Risikobewerten von Netzwerkverkehr in Unternehmen spezialisiert. Gemäss ihren Erfahrungen werden in Unternehmen heute durchschnittlich pro Monat weit mehr als 1000 Cloud-Services genutzt. Und dies nicht etwa primär in Gross-, sondern explizit auch in mittleren Unternehmen.

Durch den Einsatz mobiler Geräte, Vermischung von privater und geschäftlicher Nutzung im Firmennetz werden heute im Durchschnitt bis zu 27 Cloud-Apps pro Mitarbeiter verwendet, insbesondere in den Bereichen Collaboration, Social Media, Content Sharing und File Sharing. Auch wenn Unternehmen heute Dienste wie Dropbox oder Facebook in ihrem Firmennetz ausschliessen, gibt es Mittel und Wege, an die Dienste zu kommen oder Ersatz-Services zu nutzen. Bei der Analyse dieser Services stellt sich zudem heraus, dass vielfach mehr als 100 Dienste in Anspruch genommen werden, von denen bekannt ist, dass diese für Cyber-Attacken genutzt werden. Es werden zudem monatlich mehrere Gigabyte Daten in Cloud-Dienste verschoben, welche bekannterweise aus risikoreichen und zweifelhaften Ländern betrieben werden. Es herrscht ein regelrechter Cyber-Krieg. Während man einerseits bemüht ist, alle erdenklichen Massnahmen zu ergreifen, um gefährliche Services und Quellen zu unterbinden, rüsten sich Anbieter von solchen Diensten mit immer neuen Möglichkeiten, um an die Benutzer zu gelangen. Es sind dabei nicht bloss Fälle von Phishing-Mails oder Viren-Attacken – es sind heute vielfach gezielte Attacken auf Firmen und Einzelpersonen, um an sensitive Informationen zu gelangen. Man nennt dies sinnigerweise auch «Whaling», der gezielte Angriff auf «grosse Fische».

Die Anwender lieben die meist kostenlosen Cloud-Services und finden immer neue Wege, um an Services zu gelangen, welche aktuell vom Unternehmen noch nicht blockiert sind. Es sind daher nicht primär die Daten, welche man aus Sicht des Unternehmens bewusst in externen Cloud-Services gespeichert hat, welche in Gefahr sind. Gefährdet ist mittlerweile das gesamte System des Unternehmens, weil der Angriff über die verschiedensten Kanäle möglich ist.

Das ist heute die Realität. Wenn wir über Cyber-Risiken sprechen, dann ist es keine Frage, ob man betroffen wird – es ist eher eine Frage, wann es klingelt. Und wenn wir auch alles unternehmen, um diese High-Risk-Services in den Griff zu bekommen, wird das Unternehmen früher oder später auf dem linken Fuss erwischt. Je nach Vorfall kann dies die Existenz eines Unternehmens ernsthaft gefährden.

Prävention reicht nicht mehr aus

Es wird heute bereits sehr viel in die Sicherheit von Unternehmensnetzwerken investiert. Man schätzt, dass davon zirka 80 Prozent in der Prävention und damit Vermeidung von Sicherheitsattacken angelegt wird. Dabei wird Sicherheit noch zu stark als Aufgabe einer dafür spezialisierten Funktion innerhalb der Organisation verstanden – oder extern ausgelagert. Man kauft sich damit oft bloss eine Scheinsicherheit ein. Technische Massnahmen verhelfen oft nur zu Punktlösungen. Das System ist trotzdem löchrig wie ein Schweizer Käse.

Das Risiko, als Person oder Unternehmen durch Cyber-Attacken getroffen zu werden, steigt zunehmend. Nie war es einfacher für Cyber-Kriminelle, an ihr Ziel zu kommen. Wir müssen erkennen, dass die Tage der Implementierung von Sicherheitssystemen und sich dann zurückzulehnen, definitiv vorbei sind.

Die traditionell auf Prävention ausgerichtete Informationssicherheit genügt daher nicht mehr. Die Widerstandsfähigkeit und damit das Erkennen und entsprechend Reagieren auf Sicherheitsverletzungen wird ein Überlebensmerkmal von Organisationen in der Zukunft sein. Wenn man davon ausgeht, dass man getroffen wird – so sollte man sicherstellen, dass dies nicht zu hart geschieht. Prävention ist sicher wichtig, aber es braucht auch eine ausgeglichene Investition in die Erkennung von Attacken und in die Reaktionsmassnahmen im Ereignisfall. Das Wichtigste aber ist, dass Cyber Security – oder besser Cyber Resilience in der Agenda der Geschäftsführung einen festen Platz erhält. Das Thema darf nicht mehr den Experten alleine überlassen werden, welche in der Organisation oft nicht wirklich verstanden werden. Die Lücke des Wissens zwischen den Experten und dem Rest der Organisation ist vielfach so gross, dass die heutigen Sicherheitsmassnahmen nur zur Hälfte wirken. Der Mitarbeiter ist das höchste Gut in einer Organisation – er ist aber bezüglich der Cyber-Kriminalität auch der kritischste Erfolgsfaktor. Wenn er nicht wirklich in den Schutzprozess eingebunden und sein Bewusstsein auf die Risiken geschärft wird, bleibt er immer die grösste Schwachstelle im System.

Eine ganzheitliche Cyber Resilience

Die Widerstandsfähigkeit gegen Cyber-Attacken muss in die Firmenstrategie und in das Betriebskonzept des Unternehmens integriert werden. Mit folgenden acht Stufen kann eine Organisation sich auf das Unvermeidbare besser vorbereiten:

1. Machen Sie das Thema Cyber Security zur Chefsache. Cyber-Kriminalität ist eine Gefahr für das Unternehmen und darf nicht technischen Experten alleine überlassen werden.
2. Sind Sie sich der Verletzbarkeit Ihrer Assets und damit Ihres Unternehmens bewusst. Führen Sie dazu ein ganzheitliches Risiko-Assessment durch und erstellen Sie für Ihr Unternehmen eine Bedrohungsanalyse. Berücksichtigen Sie dabei nicht bloss technische, sondern insbesondere auch nicht technische Angriffsflächen.
3. Stellen Sie den Menschen, insbesondere Ihre Mitarbeiter, Kunden und Lieferanten ins Zentrum der Massnahmen und sorgen Sie für ein Risiko- und Verhaltens-Bewusstsein.
4. Stützen Sie sich auf bewährte Cyber-Sicherheitspraktiken ab. Dabei geht es nicht um eine einzelne Handlung oder Technik – es ist vielmehr eine ausgewogene Mischung von Präventions-, Erkennungs- und Korrektur-Aktivitäten abgestimmt mit Prozessen, Technologie und involvierten Personen.
5. Planen Sie für das Schlimmste. Sie können nicht alle Attacken verhindern – aber Sie können sich für das Schlimmste vorbereiten. Die Fähigkeit, Datenverlust zu verhindern, den Service innert kurzer Zeit wieder herzustellen und damit das Vertrauen der Kunden und Lieferanten aufrechtzuerhalten, wird zum Überlebensfaktor von Unternehmen in Zukunft.
6. Haben Sie ein spezielles Auge auf versteckte Gefahren von Drittanbietern und Geschäftspartnern. Sicherheitsbewusste Unternehmen verstehen, dass Bedrohungen hinsichtlich der Datensicherheit vor allem aus mehreren Quellen und Richtungen, auch von vertrauenswürdigen Drittparteien wie Lieferanten, Partnern und anderen assoziierten Unternehmen stammen können.
7. Beachten Sie auch die Gefahren von internen Bedrohungen. Die grösste Gefahr geht vielfach von internen Quellen aus, in aller Regel von privilegierten Accounts.
8. Stellen Sie die Cyber-Sicherheit fortlaufend sicher. Neue Mitarbeiter werden eingestellt, neue Partnerschaften gebildet und aufgelöst. Jedes Mal können neue Sicherheitsrisiken auftreten, welchen man sich laufend bewusst sein muss.

Cloud-Dienste haben ein enormes Potenzial für die weitere Digitalisierung der Geschäftsprozesse. Unternehmen müssen aber lernen, mit den Gefahren umzugehen, um den Nutzen auch nachhaltig geniessen zu können. ■

Martin Andenmatten

ist Gründer und Geschäftsführer der Glenfis AG.

www.glenfis.ch