In den Griff bekommen

Sicherheitsperformance entwickeln

Interview mit Franco Cerminara von Georg Lutz

Die Perimeter der Sicherheit verschieben sich und weiten sich aus. Auf welche Angriffstrends müssen sich KMU-Verantwortliche und Sicherheitsanbieter vorbereiten?

Wir arbeiten immer mehr ausserhalb unseres klassischen Arbeitsplatzes. Mobiles Arbeiten und «Bring Your Own Device» stellen Sie als Sicherheitsanbieter vor neue Herausforderungen. Datendiebstahl ist hier vermutlich ein besorgniserregender Trend. Können Sie die Bedrohungslage skizzieren?

Mobilität und Verfügbarkeit der Daten müssen in einem heutigen Sicherheitsdispositiv unbedingt berücksichtigt werden. Mobiles Arbeiten ist ja auch heute eine Selbstverständlichkeit. Mitarbeiter erwarten, dass sie orts- und zeitunabhängig auf Daten zugreifen und diese bearbeiten können. Für Sicherheitsverantwortliche verschiebt sich dadurch der Perimeterschutz, sprich die Trennung zwischen der internen IT und dem öffentlichen Netz. Die klare Trennung zwischen internen und externen Datenräumen gibt es schlicht nicht mehr. Es geht aber nicht nur um zusätzliche Geräte wie Smartphones oder Tablets, sondern es gilt auch die Cloudlösungen im Blick zu haben. Folglich steigen die Anforderungen an Datensicherheit im Geschäftsalltag.

Ihnen geht die Arbeit nicht aus?

Richtig. Die Herausforderungen nehmen zu. Wenn man Informationssicherheit in den Griff bekommen will, geht es darum alle Prozesse abbilden zu können. Dann gilt es Mitarbeiter die entsprechenden Kenntnisse und Instrumente in die Hand zu geben, damit sie sicher (mobil) arbeiten können und in der Cloud ein sicherer Rahmen mit klaren Zugriffsberechtigungen existiert.
Die zentrale Herausforderung ist, dass viele, gerade Verantwortliche von kleine Unternehmen, nicht wissen, wo ihre sensiblen Daten liegen und wer darauf zugreifen darf – respektive. kann.

Ich muss zunächst ein Bild erstellen, damit ich einen Überblick bekomme?

Viele Verantwortliche wissen oft gar nicht wo kritische Daten liegen.
Umgangssprachlich gesagt, muss ich zunächst wissen, wo sind welche Daten, und wer bearbeitet diese mit welcher Berechtigung. Wenn ich auf dieser Grundlage eine neue Sicherheitsstruktur geschaffen habe, dann gilt es diese Struktur auch laufend zu pflegen.

Das letzte Jahr war von einem Anstieg von Android-Schadprogrammen, neuen Computerschädlingen und eCrime-Kampagnen geprägt. Sehen sie das auch so und wenn ja setzt sich dieses Jahr dieser Trend fort?

Ja, wir haben es hier immer mit Zyklen zu tun. Zunächst geht es beim Thema Sicherheit immer nur um Annäherungswerte. 100 Prozent Sicherheit gibt es nicht. Bei Android geht es auch weniger um die Sicherheit des Produktes selbst, sondern wie Mitarbeiter damit umgehen. Mitarbeiterschulung ist hier sicher ein wichtiges Thema.
Lassen Sie mich an diesem Punkt nochmals grundsätzlicher werden.

Ich bitte darum.

Informationen sind gestern und heute ein Machtfaktor. Wenn ich als Anbieter ein spannendes Produkt oder Teile eines Produkts auf dem Weltmarkt habe, bin ich für verschiedene Akteure, die auch global agieren von Interesse. Zudem kann ich, wenn ich nicht geschützt bin, auch Einfallstor für andere Unternehmen sein, da meine Rechner gekapert sind und damit auch andere Unternehmen angegriffen werden können.

Wenn die IT-Mittel unstrukturiert ausgerollt sind, Datenhaltung nicht definiert ist und Mitarbeiter nicht sensibilisiert sind, dann bieten Sie eine grosse Angriffsfläche. Vor diesem Bild, ist es dann fast schon unabhängig, ob Sie Android, Windows Mobile oder mit anderen Betriebssystemen arbeiten. Wenn bei Ihnen die Türen für Angriffe offen sind, sind Sie verletzbar.

Jetzt stellt sich die Frage, wer hier noch Luft nach oben hat. Wem fehlt die Sicherheitssen-

Sensibilisierung von Mitarbeitern ist eine wichtige Voraussetzung für eine funktionierende Sicherheitsstrategie.

sibilität. Sind es eher die Hersteller oder wir als Nutzer?

All die Gadgets und Apps mit denen wir heute arbeiten sind auf Komfort, Einfachheit und Schnelligkeit ausgerichtet. Das ist toll und wir nutzen sie gerne. Sicherheit steht hier nicht an erster Stelle. Das Bewusstsein bei Herstellern, was Sicherheitsthemen betrifft, ist heute weitgehend vorhanden. Bei uns als Nutzer muss leider oft erst ein Schadensfall eintreten, bevor wir uns des Risikos bewusst werden.

Jetzt können Sie uns sicher noch ein praktisches Beispiel verraten?

Letztes Jahr haben wir an unserer Sicherheitsveranstaltung ein Smartphone in aller Öffentlichkeit gehackt, um aufzuzeigen wie einfach es ist, eine App zu entwickeln, Daten aus dem Smartphone auszulesen und an eine dritte Person weiter zu leiten. Diese haben wir dann frei zugänglich auf einem App-Store veröffentlicht, um es den Usern anzubieten. Natürlich haben wir die App danach gleich wieder aus dem Store entfernt.

Gibt es für Sie hier eine Unterscheidung zwischen privaten und geschäftlichen Angelegenheiten?

Was wir privat machen, liegt in unserer persönlichen Verantwortung. Bei Geschäftsdaten sollte aber eine klare Sicherheitsarchitektur, die regelmässig gepflegt wird, vorhanden sein. Das ist der Ansatz unseres Hauses. Es sollten keine schwammigen Überschneidungen vorhanden sein, insbesondere bei «Bring Your Own Device» gilt es hier klare Regeln zu definieren.

Indem ich ein Privathandy als Geschäftshandy einsetze, ohne es vorher in die Sicherheitsarchitektur ein zu pflegen?

Beispielsweise. Oder wenn Ihre Kinder dann ungeschützt Spiele drauf laden, haben Sie mit hoher Wahrscheinlichkeit ein Sicherheitsrisiko am Hals.

Cloud-Speicher sind ein weiteres Einfallstor. Dropbox und andere Speicher «in der Wolke» sind bei Nutzern beliebt, um Daten zu sichern oder auszulagern. Das ist für Cyberfreaks bares Geld. Sehen Sie das auch so?

Ja, das kann ein Einfallstor sein. Sie können als Angreifer dann Schadsoftware platzieren oder Daten missbrauchen. Aus unserer Erfahrungen ist aber auch E-Mail immer noch ein klassisches Angriffsziel. Viele Angreifer versuchen via E-Mail Schadsoftware in das Unternehmen einzuschleusen, zum Beispiel über ein entsprechendes Attachment oder einen Link auf eine gefälschte Internetseite.

> «Oft laufen heute gezielte Angriffe über einen längeren Zeitraum».

Kommunikation ist ein zentraler Punkt. Bei der Reaktion und Prävention geht es immer darum, welche Kanäle Sie wem zugestehen. Daher sind Browser, Internet und E-Mail nach wie vor die heiklen Stellen und daher ist ein zuverlässiger Perimeterschutz enorm wichtig.
Oft laufen heute gezielte Angriffe über einen längeren Zeitraum. Der Fachbegriff dazu heisst «Advanced Persistent Threats», kurz APT. Es geht hier um komplexe, zielgerichtete und effektive Angriffe auf IT-Infrastrukturen. Ziel ist möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum sensible Informationen zu bekommen. Der Aufwand, der hier betrieben wird, ist enorm. An diesem Punkt sind wir dann schon bei Industrie- und politischer Spionage angelangt, die aber wie gesagt nicht nur grosse Unternehmen oder Staaten betreffen, sondern auch kleine Unternehmen, wenn Sie interessante Daten besitzen.

An welchen Punkten sind KMU-Unternehmen besonders gefährdet?

Es gibt hier verschiedene Betrachtungswinkel. Der Perimeterschutz wird sich sicher auch in den nächsten Jahren erweitern beziehungsweise ergänzen. Sicher werden Portale besonders betroffen sein. Wenn Sie als KMU in einem Nischenmarkt erfolgreich sind, dann sollten sie besonders aufpassen, da es Akteure gibt, die Sie von diesem Markt verdrängen wollen.

Bei der Frage der Mitarbeitersensibilisierung braucht es oft psychologische Tricks. Wir werden in unserem Tagesgeschäft von Informationen überflutet. Hier sind nicht nur technische, sondern auch menschliche Filter nötig, um die wichtigsten und relevantesten Punkte heraus zu finden. Die wichtigsten Punkte nachhaltig bearbeiten, so könnte unser Arbeitsmotto zusammengefasst werden.

Können wir die Kernbotschaften des Interviews zusammenfassen?

Erstens muss man Prozesse sauber konzipieren, umsetzen und optimieren. Zweitens gilt es die Infrastruktur richtig aufzubauen und sicher zu halten und drittens gilt es den Menschen gezielt zu sensibilisieren. Wenn man alle drei Dimensionen der Informationssicherheit berücksichtigt, dann ist man auf dem richtigen Weg. ■

Franco Cerminara

ist Head of Consulting bei der InfoGuard AG.

www.infoguard.ch