



# Ein weites Feld

## Trends und Herausforderungen bei Sicherheitslösungen

Interview mit Stephan Schweizer und Tom Sprenger von Georg Lutz

Aktuell wird medial fast jede Woche ein neues Horrorszenario aufgebaut. Nehmen wir ein Beispiel: Die Kollegen von Kaspersky Lab haben eine neue Schadsoftware entdeckt. Die Virenforscher sprechen von bislang ungeahnter Komplexität und Qualität, vom «Todesstern der Malware-Galaxie». Die Stuxnet-Angriffe sollen da vergleichsweise harmlos sein. Da kommen einige wirkungsmächtige Bilder zusammen, die den Laien frösteln lassen. Inwieweit betreffen solche Meldungen durchschnittliche Schweizer KMU-Verantwortliche?

Stephan Schweizer: Es gilt hier sehr nüchtern zu bleiben und strategische Punkte zu beachten. Als KMU-Verantwortlicher muss man primär seine Hausaufgaben richtig machen. So sollte die IT-Infrastruktur auf einem aktuellen Stand gehalten werden. Es gilt die Benutzer zu instruieren und die gängigen Sicherheitsmechanismen, die ja heute schon zur Verfügung stehen, konsequent einzusetzen. Dabei muss Geld investiert werden. Sicherheit aus dem Hobbykeller reicht

schon lange nicht mehr aus. Es sollten Fachkräfte damit beauftragt werden.

**Jetzt könnte man einwenden, ich arbeite ja nicht in einem iranischen Atomkraftwerk.**

Klar. Aber es gibt viele Schweizer KMU, die sehr interessante Daten für potenzielle Angreifer haben. Der «Todesstern der Malware-Galaxie» ist allerdings nun wirklich die ganz hohe Schule der Mal-

ware. Der Aufwand für den Angreifer ist beträchtlich. Das lohnt sich nur bei «High-Value Targets».

**Woran machen Sie das fest?**

Die Malware ist sehr aufwändig programmiert und funktioniert zielgerichtet auf bestimmte Endsysteme. Sie erkennt beispielsweise selbst, ob sie ein lohnendes Ziel getroffen hat. Wenn nicht, schaltet sie sich automatisch ab.

Varianten zu tun. Das ist ein gigantisches Katz- und Maus-Spiel zwischen Angreifern und Schützern. Wir als Verteidiger können nur das bekämpfen, was wir wirklich kennen. Es gibt daher heute nur einen bedingten Schutz mit einem Virens Scanner. Er reicht für einige aus, für andere aber nicht. Wenn es um sehr schützenswerte Daten geht, dann muss man sich über Themen wie Datenverschlüsselung und restriktive Datenzugriffsrechte Gedanken machen.

Dies umso mehr, wenn neben den eigenen Mitarbeitenden auch externe Personen wie Kunden und Lieferanten auf die Kernsysteme des Unternehmens Zugriff haben.

## «Es geht um eine Awareness der Mitarbeitenden.»

**Es gibt in der Sicherheitsbranche zwei grundsätzlich unterschiedliche Herangehensweisen. Zum einen geht es um den Präventionsansatz, zum anderen um den Reaktionsansatz. Wann ist welche Strategie sinnvoller?**

Prävention heisst übersetzt, den Fokus auf vorbeugende Massnahmen zu legen. Man hat aktualisierte Systeme, genauer gesagt man lässt sie aktualisieren. Bei einem Virens Scanner muss man heute fast tagesaktuell sein. Dazu kommen die Vorkehrungen im Rahmen der Infrastruktur. Beim reaktiven Ansatz liegt die Voraussetzung darin, dass Mechanismen die Detektion ermöglichen. Zudem braucht es ein Monitoring und dann am Ende dieser Sicherheitskette Kompetenzen, damit man die nötigen Massnahmen einleiten kann.

**Das Handeln in Echtzeit erfordert aber eine Performance auf sehr hohem Niveau. Wenn ich nur an die nötige Rechnerleistung denke. Das ist auf klassischen KMU-Servern in der Besenkammer nicht zu leisten.**

Schweizer: Kommt darauf an, was man in Echtzeit haben will. Wenn man das Verhalten der Nutzer innerhalb des Unternehmens analysieren will, um sicherheitsrelevante Defizite festzustellen, trifft Ihre These zu.

**Können Sie das kurz etwas ausführen?**

Es geht zum Beispiel darum, dass der Ort und die Bewegungen von schützenswerten Dokumenten lückenlos erfasst werden. Verlässt ein schützenswertes Dokument unautorisiert per Mail das Unternehmen, schrillen die Alarmglocken. Man muss aber in jedem einzelnen Fall die Anforderungen genau anschauen, um zu einer passenden Lösung zu kommen. Mit massgeschneiderten Lösungen lassen sich die Performance-Anforderungen massgeblich reduzieren.

**Die beste technische Sicherheitsstruktur nützt mir nichts, wenn ein Mitarbeiter einen USB-Stick auf seinem Schreibtisch findet und ihn in den Rechner steckt. Wie kann die Sensibilität bei solchen Themen wachsen?**

Es braucht eine Sicherheitskultur. Um diese operativ zu implementieren, führen wir mit Unternehmen Sicherheitsprogramme durch. Nur die technische Seite abzudecken ist heute definitiv zu wenig. Es geht um eine Awareness der Mitarbeitenden. Es gilt klare Prozesse zu definieren, bei denen auch Rechte vergeben und entzogen werden.

**Oftmals ist gerade auch in der Finanzbranche der historisch gewachsene punktuelle Schutz noch vorherrschend. Betrug, Identitätsdiebstahl, Spam und Phishing nehmen in Zeiten des Onlinebanking zu. Können Sie die Bedrohungen qualitativ einordnen?**

Sprenger: Die Bedrohungssituation in der Finanzbranche ist sicherlich akuter. Es geht ja im wahrsten Sinne des Wortes um mehr Geld. Im internationalen Vergleich ist der Schweizer Finanzplatz, was das Thema Sicherheit betrifft, gut aufgestellt. Wenn wir in die einschlägigen Foren reinschauen, heisst der Tenor dort: Lasst uns die Kanonen auf andere Länder ausrichten, der Aufwand ist hier viel zu hoch. Das betrifft zum Beispiel die berühmten fingierten Transaktionsbestätigungen.

**Von der zuständigen staatlichen Stelle, dem MELANI (vergleiche. Einleitungstext in dieser Rubrik, die Redaktion), hört man aber doch immer wieder von Trojanern, die auch die Finanzbranche betreffen. ►**

**Der erste Schritt in Richtung passender Schutz ist vermutlich die strategische Bewertung meiner Daten?**

Tom Sprenger: Ja, dem stimme ich zu. Allerdings ist ein gewisser Grundschutz auf der Höhe der Zeit für alle KMU notwendig. Dabei geht es um Dinge wie die regelmässige Aktualisierung der Software oder eine saubere Perimetersicherheit. Es gibt heute zwei Möglichkeiten. Entweder schafft man selbst den Rahmen auf lokaler Ebene oder man geht in eine professionelle Cloud-Lösung.

**Wo liegen die Risiken einer klassischen Sicherheitsarchitektur?**

Heute läuft fast die gesamte Malwareproduktion auf einem sehr hohen Niveau ab. Schauen Sie sich nur die aktuellen Zahlen der Mutationen an. Inzwischen haben wir es mit Hunderten von Millionen unterschiedlicher Schadsoftware-





Manchmal kann der Diebstahl nicht verhindert werden, aber der anschliessende Missbrauch.

Meine Aussage heisst nicht, dass die Verantwortlichen die Hände in den Schoss legen können. Es gibt tatsächlich Trojaner, die gezielt für E-Banking-Lösungen gebaut und eingesetzt werden. Das ist effektiv ein Thema. Mit unseren Lösungen adressieren wir den Themenkomplex auf verschiedenen Ebenen. Die grundsätzliche Stossrichtung ist die, dass wir neben der Perimetersicherheit auf einem höheren Abstraktionslevel Anomalie-Erkennung betreiben. Selbst sehr gut getarnte Trojaner verhalten sich anders als ein Mitarbeiter. Das kann man erkennen.

### Was heisst das praktisch?

Man analysiert, wie sich der Nutzer innerhalb der Applikation bewegt. So erhält man einen Navigationsablauf. Der Benutzer wählt innerhalb der Applikation einen üblichen Pfad, weicht er davon ab, gilt es genauer hinzuschauen. Beim Thema Identitätsdiebstahl kann man aktuell Lücken nicht ausschliessen. Da wird gerade im privaten Bereich doch auf einen Link geklickt, die Hardware dann aber auch im Unternehmen eingesetzt.

### Das ist die Sicherheitsherausforderung bei Bring your own Device?

Richtig. Daher lautet der Ansatz hier wie folgt: Wenn man den Diebstahl schon nicht verhindern kann, dann wenigstens den Missbrauch. Dort helfen intelligente Autorisierungssysteme weiter. Diese erkennen, dass potenziell eine gestohlene Identität verwendet wird, und notifizieren den rechtmässigen Besitzer. Dieser hat dann die Möglichkeit, einzugreifen, indem er die verdächtige Verwendung der Identität (Session) terminiert.

**Es geht, um die grundsätzlichen Ansätze nochmals zusammenzufassen, nicht nur um präventive und reaktive Möglichkeiten, sondern man kann drittens auch nach dem Schadensfall die Situation bearbeiten?**

Ja. Gerade beim Thema Identitätsdiebstahl kann der Zeithorizont zwischen dem Diebstahl und dem Auffallen des Verlustes sehr weit sein. Die Idee ist hier, dass man den Nutzer schon bei Verdacht in die Reaktionskette miteinbezieht.

### Was wird sich in den Bedrohungsszenarien in den nächsten Jahren tun? Wagen Sie eine Prognose?

Die Erfahrungswerte geben leider keinen Anlass zur Entwarnung. Die Bedrohungen werden zunehmen. Es gibt dafür eine ganze Branche, die weltweit sehr gut aufgestellt ist und Produktion und Vertrieb professionell betreibt. Die werden nicht so schnell die Flinte ins Korn werfen. Heute kann man Malware für verschiedenste Zwecke und Zielgruppen problemlos einkaufen.

Schweizer: Die meisten Banken wollen heute ihre Kunden auf verschiedenen Kommunikationswegen erreichen. Das führt zu einer Ausweitung der Sicherheitsbedrohungen. Insbesondere die mobilen Kommunikationskanäle werden davon betroffen sein.

Sprenger: Das mobile Gerät ist ein High-Level Target. Dort hat der Benutzer seine gesamte digitale Identität gespeichert. Wenn man ihn umfassend schädigen will, dann liegt man hier richtig.

Schweizer: Die klassische Perimeter-



sicherheit erodiert. Durch die zunehmende Verbreitung von Cloud-Lösungen und mobilen Geräten ist die klassische Mauer löchrig geworden. Man braucht sie in der Zukunft trotzdem, sie reicht aber nicht aus. Man wird eine neue Generation von Sicherheitslösungen bauen müssen. Dabei geht es

nicht nur um Abschirmung, sondern um Beobachtung von auffälligem Verhalten.

### **Jetzt kommen Anbieter wie AdNovum mit einer Managed Security ins Spiel?**

Es gibt bei uns auch Produkte zu kaufen. Es geht nicht nur um Dienstleistungen.



Die klassische Perimetersicherheit erodiert.

gen. Aber klar, wir wollen die ganze Kette abdecken. Das betrifft zum Beispiel die Sicherung von Webportalen, die Datenfilterung auf dem Kommunikationskanal, die Sicherstellung der Authentifizierung und das Identitätsmanagement. Diese standardisierten Lösungen brauchen meist ein kleines Integrationsprojekt. Alternativ können sie Teil einer Gesamtlösung sein, bei der von uns auch Applikationen entwickelt werden.

### **Bei Ihnen läuft das unter dem Stichwort «CIO as a Service». Da kann ich mir mein passendes Paket zusammenstellen. Das betrifft auch KMU?**

Schweizer: Wir können die Bausteine dieses Ansatzes bei KMU implementieren. Das ist auch für kleine Unternehmen sehr attraktiv. Sie beziehen das als Service innerhalb einer Cloud-Lösung. Da braucht es einen sicheren Cloud-Provider. Das Auslagern der CIO-Funktion macht für viele KMU Sinn. Daher auch unser Motto: «CIO as a Service». ■



**Stephan Schweizer**

ist Nevis Product Manager bei der AdNovum Informatik AG und in dieser Rolle auch für strategische Kundenprojekte verantwortlich.



**Dr. Tom Sprenger**

ist seit 2013 CTO der AdNovum Firmengruppe. Davor hat er als CIO den Aufbau der globalen IT-Infrastruktur von AdNovum vorangetrieben.

[www.adnovum.ch](http://www.adnovum.ch)