Ich könnte das nächste Ziel sein

Sicherheitsstrategien umsetzen

Interview mit Franz Kaiser von Georg Lutz

Ende Juni ist Hoststar, ein Schweizer Provider und KMU, massiven Angriffen ausgesetzt gewesen. Dies ist nur ein Beispiel, dass die Notwendigkeit von der Etablierung von strategischen Sicherheitskulturen in kleineren Unternehmen verdeutlicht.

Einer der zentralen Begriffe Ihres Kerngeschäfts heisst Unified Threat Management (UTM). Lassen Sie uns das für IT-Laien übersetzen. Früher gab es viele spezialisierte Sicherheitslösungen, heute kann von einer Plattform aus gehandelt werden. Kann man dies so zusammenfassen?

Grundsätzlich Ja. Früher hatte man eine Lösung für die Firewall, eine für die Verschlüsselung oder die Anti-Virusproblematik. Zudem bezog man diese Angebote oft auch noch von unterschiedlichen Herstellern. Gerade im KMU-Bereich stösst man dabei schnell an Grenzen …

… Es gibt ja keine eigene IT-Abteilung.

Genau. Meist gibt es nur einen Verantwortlichen und der wird schon im Tagesgeschäft aufgerieben. Er muss zum Beispiel abgestürzte PCs wieder zum Laufen bringen. Er kann sich viel zu wenig um die Angebote der Hersteller kümmern. Das ist der Ausgangspunkt für UTM. Es gibt nur eine Hardware und auf der sind alle Lösungen von einem Anbieter vorhanden. Solch einen Weg haben wir auch eingeschlagen.

Eine grosse Herausforderung im Rahmen aktueller Sicherheitsstrategien sind mobile Arbeitsgeräte im Geschäftsalltag. Bringt das Stichwort «Bring your own Device» Sie als Sicherheitsmensch nicht zur Verzweiflung?

In der Vergangenheit stellte die Firma dem Mitarbeiter Geräte zusammen, die er in dem Unternehmen nutzen konnte. Wenn ich als Unternehmen die Geräte zur Verfügung stelle, kann ich dementsprechend Sicherheitslösungen auf die Notebooks oder Smartphones installieren und dementsprechend zentral managen. Bei «Bring your own Device» funktioniert das nicht. Die Geräte gehören den Mitarbeitern und als Firmenverantwortliche habe ich darauf keinen Zugriff. In der Folge wachsen bei IT-Verantwortlichen die grauen Haare.

Wie kann man das verhindern?

Wenn ich nicht mehr auf den End-Client zugreifen kann, muss man die Lösung im Netzwerk suchen. Das ist unser Ansatz. Wenn der Client versucht, im Netz Daten zu holen, oder aus dem Netz Mails zu verschicken, dann können wir das kontrollieren. Wir wissen dann beispielsweise, dass dies sein iPhone ist und welcher der User tätig ist. Das Unternehmen kann dann entsprechend Firmen-Richtlinien setzen. Wenn zum Beispiel Herr Meyer mit seinem von der Firma gestellten Notebook kommt, erhält er eine grüne Ampel. Wenn Herr Meyer aber mit seinem privaten iPad kommt, dann muss die volle Ladung an Sicherheit zur Anwendung kommen. Wir fliegen sonst hier im Sicherheitsblindflug und haben keine Ahnung, was er so macht. Ausgangspunkt ist: Wir erkennen automatisch das Gerät mit Betriebssystem, den Benutzer und die Applikation in Realtime. Dies erlaubt den Sicherheitsverantwortlichen entsprechende Rules zu setzen , um grösstmögliche Sicherheit zu garantieren.

Wobei da es ja nicht nur um technologische Lösungen geht, sondern um die Umsetzung einer Sicherheitskultur im Unternehmen. Da sind Sie und Ihre Vertriebspartner tätig?

Ohne Frage ist Social Engineering eine der Hauptherausforderungen bei der Umsetzung von Sicherheitsstrategien. Wir kennen alle die Beispiele mit den USB-Sticks.

Verraten Sie uns doch noch ein drastisches Beispiel?

Wer auf einem Firmenparkplatz einen USB-Stick mit der Aufschrift «Gehaltsliste» platziert, hat grosse Chancen, dass der USB-Stick auch in einem Firmenrechner landet. Und schon hat man sich einen Trojaner eingefangen Das passiert nur dann nicht, wenn dort auf allen Hierarchieebenen eine Sicherheitskultur gelebt wird. Die Mitarbeiter müssen in den Grundzügen die Vorgehensweise von Hackern kennen. Nur dann kann uns Technologie auch wirklich weiter helfen.

Kommen wir zu einem weiteren wichtigen Stichwort: Client Reputation. Die Reputation eines Unternehmens in der HR Welt bezieht sich auf gute Beziehungen zwischen dem Unternehmen und seinen Stake- und Shareholdern. Inwieweit kann man diese in die IT-Welt hinein übersetzen?

Bleiben wir beim Beispiel unseres Herrn Meyer. Unser Gerät erstellt ein Baselining, das erkennt, wie viele E-Mails Herr Meyer typischerweise versendet, auf welche interne IP-Adressen er zugreift und welche Webseiten er normalerweise besucht. Dabei interessiert mich nicht die konkrete Webseite, sondern die Webseite passt in ein Kategorie-Raster. Sollte er sehr oft auf Seiten sein, die aus Tonga stammen, geht seine Reputation nach unten. Auch bei gewissen chinesischen oder russischen Seiten muss er mit einer Abstufung rechnen. Ich muss annehmen, dass er Files herunterlädt, von denen auch üblicherweise Angriffe gestartet werden. Auffällig wird Herr Meyer auch, wenn er plötzlich sehr viel mehr E-Mails als sonst schreibt. Oder er sendet grosse Datenmengen an eine spezifische Webseite, dann müssen wir eingreifen. Oder er versucht unerlaubte DNS-Auflösungen oder ähnliches. Bei der Client-Reputation geht es um eine Behavior-Analyse jedes Clients.

Sie wollen aber nicht Herrn Meyer überwachen?

Es geht um eine Art Ranking, bei der ab gewissen Punkten unsere Alarmglocken schrillen. Es interessiert uns überhaupt nicht, ob Herr Meyer fünf Minuten auf der Blick-Seite war, oder die Öffnungszeiten seines Fitnessstudios in Erfahrung bringt. Das ist völlig unwichtig und geht niemand anderen etwas an. Es geht darum, ob er sich auf Seiten bewegt, die für Malware bekannt sind oder in einer Art und Weise agiert, was auf eine Botnetz-Infizierung hinweisen könnte.

Wie sehen die aktuellen Trends bei den Attacken aus? Muss man mit länderspezifischen Angriffen rechnen?

Ja, das ist ein wichtiger neuer Trend. Dieser Trend hat auch einen Namen. Er heisst Advanced Persistent Threat (APT). Es geht um zeitlich langfristige und andauernde Bedrohungen. Um was geht es hier? Um die zunehmende Professionalisierung der Szene. Wir reden ja nicht mehr von pubertierenden Jugendlichen im Keller, die einen Virus entwickeln, sondern um Geschäftsmodelle mit viel Wissen, Macht und Geld im Hintergrund. Das heisst, die Zielgenauigkeit nimmt zu. Es sollen im Rahmen von Wirtschaftsspionage gezielt Firmen angegriffen werden. Das passiert auch in der Schweiz. Es gibt gerade in der Schweiz sehr viele KMU, die im internationalen Vergleich sehr gut da stehen, die teilweise sogar Leader sind. Deren Firmendaten sind ausländischen Unternehmen Gold wert.

Können Sie uns noch ein konkretes Beispiel verraten?

Ende Juni ist zum Beispiel Hoststar, ein Provider, bei dem ich meinen privaten Webauftritt habe, grossflächig angegriffen worden. Hoststar hat sich äusserst professionell verhalten, transparent informiert und schnell agiert. Aber, und das ist der Punkt, Hoststar ist kein riesiges Unternehmen in der Schweiz, sondern eine KMU und wurde gezielt angegriffen.

Inzwischen gibt es nicht nur böse russische Netzwerke und Chinesen, die an unsere Firmendaten gelangen wollen, sondern es sind die NSA oder Programme wie PRISM in den öffentlichen Focus gerutscht. Bekommen Sie als kalifornischer Anbieter Anrufe von Schweizer Kunden, die sich um ihre Daten sorgen?

Bisher noch nicht. PRISM prüft den internationalen Datenverkehr, wenn er über die USA läuft. Da ist ein Schutz sehr schwierig, wenn der Internetprovider in den USA es zulässt, dass es eine externe Box gibt, die die Daten abschöpft. Auch in Europa ist dies in Teilen der Fall. Jetzt kann man den Datenverkehr grundsätzlich verschlüsseln, dann wird es schon sehr viel schwieriger. Irgendwann lohnt sich da der Aufwand nicht mehr. Wenn sich PRISM bei einem Unternehmen in der Schweiz Daten holen will, sind wir wieder beim Thema Client Reputation. Sobald ungewöhnliche Aktivitäten in dieser Richtung von unseren FortiGates erkannt werden, geht die Client-Reputation stark nach unten, die Sicherheitsverantwortlichen des Unternehmens werden alarmiert und, wenn nötig, wird die Kommunikation unterbrochen. ■

Franz Kaiser

ist Regional Director Austria & Switzerland von Fortinet.

www.fortinet.com