



Ganzheitliche Betrachtung

Sicherheitslücken im Griff

Interview mit Andreas Wisler von Georg Lutz

Jenseits des medialen Getümmels um Datenskandale im Rahmen von Cyber Crime und Cyber War, stellt sich die Frage wie Unternehmensverantwortliche in ihrem betriebswirtschaftlichen Umfeld agieren sollen. Das Hauptaugenmerk sollte sich auf Schwachstellen in der Sicherheitsarchitektur richten, um Probleme zu entdecken und geeignete Massnahmen zur Behebung aufzuzeigen.

Wer als Unternehmensverantwortliche, gerade von kleineren Unternehmen seine IT-Sicherheit neu aufstellen will, steht vor einem Berg vor Herausforderungen. Früher hatte man eine Firewall und ein Antivirenprogramm. Heute kann man jeden Tag von komplexeren und gefährlichen Bedrohungen lesen. Welche Überlegungen sind dabei wichtig und welche eher unwichtig?

Es ist richtig, professionelle Kriminelle haben den Weg in das Internet gefunden und bedrohen uns auf verschiedenen Wegen. Ein aktueller und zuverlässiger Perimeterschutz ist dabei immer noch ein sehr wichtiger Baustein. Firewall und E-Mail Schutz sind auch heute noch zentrale Stichworte. Dann geht es um den Datenschutz, sprich eine Sicherheitsarchitektur, bei der klar ist wer, wann auf welche Daten zugreifen darf. Zudem müssen die Daten selbst, schon aus rechtlichen Gründen, sicher gespeichert werden. Wenn ein Sicherheitsvorfall eintritt, ist es ja für die Funktionsfähigkeit meines Unternehmens ganz wichtig, dass ich möglichst schnell wieder Zugriff auf meine Daten habe und sie sicher intern und extern austauschen kann.

Das geht bis hin zu der Aufforderung seine Daten extra zu verschlüsseln. Was halten Sie da-

von? Das ist ja sehr aufwendig.

Verschlüsselung ist ein schwieriges und komplexes Thema. Für viele Anwender sind diese Anforderungen zu hoch. Sie können das Verschlüsselungsthema nicht bis zum einzelnen Mitarbeiter eines KMU-Unternehmens herunter brechen. Das muss zentral, beispielsweise über einen E-Mail-Proxy gelöst werden.

Ihr Haus bietet in ihrem Sicherheitsangebot einen «IT-Security Audit» an. Was hat man sich darunter vor zu stellen?

Wir haben zwei Arten von Sicherheitsaudits. Es geht zunächst um ein technisches Audit, wir nennen das «Quick Audit». Wenn jemand schnell wissen will, wo man in Sicherheitsfragen steht, ist



Einfache Ziele werden angegriffen.

dies das richtige Werkzeug. Dort interessieren uns Geschäftsprozesse nur am Rande. Wir analysieren Server, Clients, Netzwerk und Firewall. Dort zeigen wir dann Schwachstellen auf und präsentieren dem Kunden mögliche Schlussfolgerungen und Lösungsmöglichkeiten.

Und beim umfassenderen Angebot, wie sieht da das Vorgehen aus?

Beim «IT-Security-Audit» gehen wir weiter. Dort geht es auch um eine Analyse der Geschäftsprozesse und wie diese mit Sicherheitsanforderungen kommunizieren. In diesem Fall gibt es umfassende Interviews mit der Geschäftsleitung, den IT-Verantwortlichen und einigen Mitarbeitern. Daraus kann dann beispielsweise auch ermittelt werden, welche Daten wirklich wichtig sind. Mit einer neuen Sicherheitsstruktur, die das gesamte Unternehmen umfasst, können dann auf einer sicheren Grundlage ein Massnahmenkatalog entwickelt werden.

Die Kunst besteht darin, technische Herausforderungen mit denen aus der HR-Abteilung zu verknüpfen?

Die Mitarbeiter, die mit den Lösungen arbeiten, in das Boot mit rein zu holen, ist enorm wichtig. Es geht darum sie in die Prozesse mit einzubinden, es muss klar werden, warum wir etwas so machen. Es ist der falsche Weg, Mitarbeiter vor vollendete Tatsachen zu stellen. Zudem geht es darum, auch Hilfsmittel zur Verfügung zu stellen. Das beginnt bei ganz banalen, aber wichtigen Sachen, wie zum Beispiel der Erstellung eines Passwortes.

Angesichts immer neuer Bedrohungsszenarien, die auch oft nicht immer sofort erkannt werden, sind IT-Verantwortliche oft überfordert und fühlen sich wie im Hase und Igel Spiel wenn sie versuchen immer neue Löcher zu

stopfen. Wie stellt sich die Situation aus Ihrer Sicht dar?

Aus meiner Sicht werden in erster Linie die Ziele angegriffen, die auch einfach erreichbar sind. Wenn ich einen guten Basisschutz habe, kann ich zwar immer noch im Fokus sein, die direkte Bedrohung nimmt aber ab. Der Ausnahmefall wäre dann gegeben, wenn ich zum Beispiel etwas entwickelt habe, dass in dieser Form niemand bisher auf dieser Welt entwickelt hat. Dann bin ich automatisch auf dem Radarschirm von Hackern und sollte mir zusätzliche Strategien überlegen, die dann auch mehr kosten. Das ist aber nicht der Alltag.

Was ist Alltag?

«Es braucht zudem Sensibilisierungsmassnahmen für Mitarbeiter».

Das ist eine aktuelle Firewall und Virenschutz, die gepflegt werden muss. Es braucht zudem Sensibilisierungsmassnahmen für Mitarbeiter. Dabei geht es nicht um eine Veranstaltung bei der Implementierung einer neuen Software, sondern um regelmässige Gespräche mit den Mitarbeiterinnen und Mitarbeitern, damit sich im ganzen Unternehmen eine Sicherheitskultur entwickelt.

Als praktische Konsequenz aus den Bedrohungen haben Sie einen «Penetrations-Test» entwickelt. Was passiert dabei?

Rubrik

Wir gehen dabei wie ein potenzieller Hacker vor. Wir brechen von aussen ein und versuchen Schwachstellen aufzuspüren und auszunutzen und schauen dann wie weit wir in die Datenstruktur des Unternehmens eindringen können. Das kann über einen Scan an der Firewall funktionieren, bei dem wir die Löcher in der Firewall ermitteln können. Auch der E-Mail- oder Webserver haben oft Schwachstellen. Die Webseite selbst kann ebenfalls manipuliert werden. Das sind simulierte Angriffe von aussen, bei denen Unternehmensverantwortliche oft überrascht sind, wie einfach ein Einbruch stattfinden kann.

Viele werden sich fragen: Lohnt sich der Aufwand. Ich bin doch nicht der Betreiber einer iranischen Atomanlage?

Es ist richtig, wir hören oft den Satz: «An meinen Daten hat niemand Interesse». Diese Aussage ist heute schlicht falsch. Schauen wir uns den Schweizer Markt an. Die Schweizer Volkswirtschaft ist sehr innovativ, wir melden immer noch die meisten Patente an, bei uns gibt es sehr viel Wissen. Für dieses Wissen sind einige Akteure bereit sehr viel Geld auszugeben und Energie zu investieren. Daher gilt es sich davor zu schützen.

Sonst sehe ich mein Produkt irgendwo auf der Welt und bin völlig überrascht.

Ja, das sieht man dann zum Beispiel in der Automobilindustrie.

Können wir hier ein Fazit wagen?

IT-Sicherheit ist kein Thema, dass man nebenbei betreiben kann. Es ist ein stetiger Prozess, bei der auch die Geschäftsleitung Verantwortung tragen muss. Die Strategie zu sagen «IT, jetzt mache mal voran und zeig was» ist falsch. Die Experten, die Geschäftsleitung und jeder einzelne Mitarbeiter müssen in einen Sicherheitsprozess mit eingebunden werden. ■



Andreas Wisler

ist IT Spezialist bei GO OUT Production GmbH, welche sich mit umfassenden Security-Audits, Penetration-Tests und Sicherheitsberatungen auseinandersetzt.

www.goout.ch
www.goSecurity.ch