

25.07.11

Von: Kolaric

## Barclay Technologies: Ergeben sich spezielle Anforderungen für den öffentlichen Sektor?



Kilian Zantop

Generell war es in der Vergangenheit für den öffentlichen Sektor viel schwieriger, im Bereich der IT-Sicherheit mitzuhalten

Je wertvoller die gespeicherten Informationen eines Unternehmens, desto größer ist das Risiko für einen Angriff.

Sony, Barracuda, Lockheed Martin Corporation, Citibank, IWF, Weißes Haus und andere sind allesamt Unternehmen und Institutionen, deren Netzsicherheitssysteme auf höchste Sicherheit getrimmt sind. Trotzdem führte beispielsweise eine SQL-Injection-Schwachstelle bei Barracuda zu massiven Datenverlusten. Hacker entwenden Informationen über die Zwei-Faktor-Authentifizierungsprodukte von RSA – deren Kunden „sitzen auf dem Trockenen“. Es folgte ein Einbruch in das Sicherheitsnetzwerk des Rüstungskonzerns Lockheed Martin – was da entwendet wurde, kann man sich denken. Kontrollinstrumente und exzellent ausgestattete Sicherheits-Teams schützen vor den unterschiedlichsten Störfallszenarien und dennoch nutzen alle diese technischen Maßnahmen nichts.

Häufig kommen von den auf IT-Security spezialisierten Unternehmen interessante Empfehlungen wie:

- „Die Unternehmen sollten ihre Strategien zum Schutz digitaler Daten überprüfen.“
- „Die IT-Sicherheitsstrategie sollte in Zukunft ebenfalls zum Aufgabengebiet des Top-Management gehören.“
- „Das Risikoprofil des Unternehmens sollte unter die Lupe genommen werden.“
- „Neue IT-Bedrohungen erfordern ein Umdenken beim Schutz der Daten.“

## **Die Aussagen klingen oft sehr vernünftig, doch was genau verbirgt sich dahinter? Wie können sich Unternehmen – ausgehend von der aktuellen Bedrohungslage – besser vor Angriffen schützen? Was können Unternehmen tun, wenn selbst namhafte IT-Sicherheitsanbieter erfolgreich gehackt werden konnten?**

Das größte Problem ist nach wie vor der „normale Benutzer“ und sein Verhalten. Dies ist leider auch bei spezialisierten Unternehmen der Fall, da auch dort „IT-ferne“-**Sachbearbeiter** wie z.B. Buchhalter arbeiten. Deren IT-Bewusstsein sollte einen viel größeren Stellenwert haben. Risiken in Bezug auf die IT werden dadurch zwar nicht völlig ausgeschlossen, aber sie lassen sich doch erheblich verringern. Ein weiterer Aspekt ist meistens auch, dass notwendige und sinnvolle IT-Maßnahmen nicht umgesetzt werden, weil der Sicherheitsverantwortliche zu wenig organisatorische Entscheidungsbefugnis hat.

## **Kann man sich überhaupt noch gegen Hacker schützen?**

Hacker nutzen heutzutage oftmals **APTs (Advanced Persistent Threat)**, um Informationen/Daten aus Unternehmensnetzwerken entwenden zu können. Die Wahrscheinlichkeit, Opfer eines APTs zu werden, ist für „normale“ Unternehmen noch immer relativ gering. Meistens werden auf diese Art und Weise Unternehmen angegriffen, welche im Fokus der Öffentlichkeit stehen oder jene, bei welchen sehr begehrte Informationen in lohnenswerter Größenordnung zu entwenden sind. Tatsächlich sind nur solche gezielten Angriffe sehr schwer zu entdecken und zu verhindern. Um alltäglicheren Angriffen entgegenzuwirken, sollten auf jeden Fall „**State of the Art**“ Technologien zum Einsatz kommen. Unter „State of the Art“ Technologien sind Firewall, Datensicherheits-/Datenverschlüsselungslösungen, Anti Virus, Strong Authentication, Intrusion Prevention/Intrusion Detection Systeme, PKI, Log und Alert Management, VPN und weitere Maßnahmen zu verstehen.

## **Hinken die auf IT-Sicherheit spezialisierten Unternehmen dem Hacker-Know-How hinterher?**

Wenn dies überhaupt der Fall ist, dann nur unwesentlich. Das Problem ist viel eher, dass es nur sehr wenig richtig gute Spezialisten gibt und deren Ratschläge und Produkte selten komplett und korrekt umgesetzt werden. Weiter sind sich viele Anwender/Kunden nicht bewusst, dass IT Security keine einmalige Sache ist, sondern eine permanente Aufgabe darstellt. Diese besteht aus kontinuierlichem Überprüfen des Ist/Soll-Vergleichs und entsprechenden Erweiterungen und Korrekturen vorhandener Schutzlösungen, da sich die Bedrohungslage fortlaufend weiterentwickelt und verändert. Ebenso gehört das Ziel, sprich die Soll-Definition, immer wieder hinterfragt und korrigiert.

## **Ergeben sich spezielle Anforderungen für den öffentlichen Sektor?**

Generell war es in der Vergangenheit für den öffentlichen Sektor viel schwieriger, im Bereich der IT-Sicherheit mitzuhalten, da die Strukturen träger sind als beispielsweise in Unternehmen der Privatwirtschaft. Dies machte es schwierig die notwendigen Spezialisten zu beschäftigen und auch die geeigneten Maßnahmen zeitgerecht umzusetzen. Deshalb müssten dort entsprechende Ausnahmen in den Strukturen geschaffen werden, da die Daten, welche dieser Sektor pflegt, besonders sensibel sein können.

**Bei der Recherche einiger auf unserer Webseite erschienenen Artikeln stießen wir auf sehr unterschiedliche Aussagen. Ein Teil der IT-Security-Verantwortlichen auf der Herstellerseite behaupten, die Angriffe sind auf die Netzwerk-Infrastruktur ausgerichtet. Ein anderer Teil behauptet, Exploits, also Schadprogramme, die Software-Sicherheitslücken ausnutzen, zielen dabei zunehmend direkt auf Dateien, Datenbanken oder Anwendungsserver ab – nicht auf die Netzwerk-Infrastruktur, auf die Unternehmen bisher ihre Sicherheitsbemühungen konzentriert haben.**

## **Was meinen Sie? Welche mehrschichtigen Ansätze wären notwendig? Was machen Unternehmen in Bezug auf die Sicherheit im Netz falsch?**

Logischerweise sehen Hersteller den Bedarf immer dort, wo sie eine Lösung bieten können. Generell ist durch die technologische Entwicklung, das Spektrum der Angriffe definitiv breiter geworden. Außerdem eröffnen sich durch neue Technologien auch immer wieder neue Möglichkeiten zum Angriff. Vor etwa 5 Jahren waren Angriffe über Smartphones noch sehr unwahrscheinlich, weil die Möglichkeiten und die Verbreitung noch zu klein waren. Grundsätzlich gilt, meiner Meinung nach, immer noch der Maßstab der Verhältnismäßigkeit. Der Schutzaufwand soll nicht mehr kosten als die Kosten des Vorfalls, den er verhindern soll. Darauf aufbauend muss man sich heute allerdings mit sehr vielen Bereichen beschäftigen. **Was machen Unternehmen nun wirklich falsch?** Sicherheit im Netz fängt bei den Menschen an, geht über die Organisation und die Prozesse, bevor sich der Kreislauf beim Netz selbst schließt. Meinen Erfahrungen nach, fehlt es in den meisten Unternehmungen an der ganzheitlichen Sichtweise. Das Beispiel „DLP“ zeigt, dass dies nicht nur eine Aufgabe für die IT darstellt. Diese ist allenfalls mit einem Großteil der Umsetzung beteiligt. Die Basis dazu müssen allerdings viele andere Unternehmensbereiche beisteuern. So können etwa nur die Ersteller/Besitzer der Daten deren Wert wirklich beurteilen. In weiterer Folge muss diese Sicht dann aber nochmals aus Gesamtfirmenperspektive aggregiert werden. Dazu kommt ebenfalls die fehlende Sensibilisierung des Business für die Risiken.

Früher galt die Regel, dass keinerlei Daten auf einen öffentlichen Webserver gehören, welche man nicht sowieso veröffentlichen will. Aus Komfort, Konkurrenz oder anderen Businessanforderungen werden jedoch immer wieder Daten an Orten gelagert oder zugänglich gemacht, wo man sie technisch einfach nicht mehr schützen kann. Das haben verschiedene Vorfälle in der Vergangenheit gezeigt.

Bezieht man sich auf die Devise „**back to the roots**“, sollte im Sinne einer ganzheitlichen Betrachtung auch darauf eingegangen werden, ob etwas sinn- und wertvoll ist. **Nur weil es technisch möglich ist, heißt das nicht automatisch, dass es auch sinnvoll ist.** Wir tendieren heute dazu, vieles zu wollen und zu machen, nur weil es geht. Dies gilt insbesondere für die Verfügbarkeit von Daten in/von Firmen zu jeder Zeit und jedem Ort, ohne Rücksicht auf Verluste - und das im wahrsten Sinn des Wortes. Deshalb sollte man einen Schritt zurücktreten und genau analysieren, was im täglichen Umgang mit den Kunden, wirklich wie viel Nutzen bringt. Man wird feststellen, dass die Anforderungen sehr viel geringer sind, und Firmendaten auch viel einfacher zu schützen sind, als oftmals angenommen. Im Falle einer einfacheren Lösung, könnte der Rest an damit gesparter Zeit, besser für den Menschen verwendet werden. „User Awareness“ kann nicht nur den Kunden oder den Mitarbeiter glücklich machen. Zufriedene Mitarbeiter sind loyaler und viel vorsichtiger im Umgang mit Firmengeheimnissen, als Mitarbeiter denen das Bewusstsein um die Sensibilität der Daten fehlt.

*Barclay Technologies, Kilian Zantop, Chief Technical Officer*