Die Gefahr kommt von Innen

IDG Business Media GMBH, 01.03.2011

Natalya Kaspersky leitet den Verwaltungsrat der Kaspersky Labs und hat bei InfoWatch den CEO-Posten inne. Dort steht der Verlust vertraulicher Daten im Unternehmen, also Data-Leakage-Protection (DLP) im Mittelpunkt des Interesses. Im Gespräch mit COMPUTERWOCHE hat sie dieses Thema näher beleuchtet.

CW: Wo sehen Sie die größten Sicherheitsbedrohungen im Internet?

Kaspersky: Ich möchte hier zwischen internen und externen Bedrohungen unterscheiden. Diese hängen zwar zusammen, aber sie finden in unterschiedlichen Regionen statt. Bei Bedrohungen von außen wollen Angreifer in erster Linie Geld verdienen. Unglücklicherweise organisieren sie sich dafür immer besser. Sie arbeiten in verschiedenen Hierarchiestufen. Der Angreifer ist nicht mehr zwangsläufig derjenige, der abkassiert. Dadurch wird es schwieriger, sie dingfest zu machen.

Interne Bedrohungen gehen auf die eigenen Mitarbeiter zurück. Diese verlieren oder veruntreuen Informationen. Wenn jemand sein Laptop am Flughafen vergisst, ist das zwar keine Absicht, aber dennoch bitter. Passiert es absichtlich, ist es ähnlich wie bei externen Bedrohungen. Angestellte versprechen sich davon monetären Gewinn. Hacker versuchen auch Mitarbeiter zu korrumpieren.

CW: Um sie als Türöffner für die Unternehmens-IT zu gewinnen?

Kaspersky: Genau. Das kann ein Systemadministrator sein, oder einfach nur jemand, der weiß, wo sich relevante Informationen befinden. Daraus können gefährliche Situationen entstehen. Wenn jemand ein Foto eines Bildschirms mit dem Handy schießt, hilft die beste elektronische Sicherung nichts.

CW: Wodurch fließen die meisten Daten ab?

Kaspersky: Mittlerweile nutzt jede Firma Antiviren-Tools und Firewalls, wodurch ein Großteil der Malware entdeckt wird. Was internen Datenverlust anbelangt, nehmen die Bedrohungen zu. Bis vor zwei Jahren war Software rar, die sich dem Problem widmete. Wir von InfoWatch setzen hier mit unseren professionellen Lösungen an. Aber auch wir stecken mitten in einer Entwicklung und müssen mit den Angreifern Schritt halten.

CW: Was ist der beste Weg, internen Bedrohungen zu begegnen?

Kaspersky: Eine Software allein kann das Problem nicht lösen. Es muss ein ganzer Maßnahmenkatalog zusammenkommen. In den meisten Unternehmen ist nicht geklärt, welche Informationen vertraulich sind und es gibt keine Regeln für den Umgang mit denselben. Wer hat Zugang? Nach welchen Regeln erfolgt der Kontakt? Das muss zuerst geklärt werden. Wer weiß, welche Informationen er schützen will, ist bereits in einer besseren Position.

CW: Sicherheitsdefizite basieren oft auf der Willkür oder der Unkenntnis der Anwender. Wie lässt sich dem begegnen?

Kaspersky: Generische Regeln für den Umgang mit vertraulichen Informationen sollten mit technischen Mitteln zusammenspielen. Wenn jemand beispielsweise Informationen auf einen USB-Stick ziehen oder per E-Mail verschicken will, sollte das geblockt werden. Das bedeutet auch, dass jemand die Verantwortung übernehmen muss festzulegen, wie vertrauliche Informationen zu handhaben sind. Jeglichen Informationsfluss zu stoppen wäre sicher ein Fehler. Es sollte nur garantiert sein, dass alle Aktionen in einer Datenbank abgelegt werden. Im Zweifel könnte sogar eine Person über den letzten Schritt beim Informationstransfer wachen. Das hätte aber eine Flaschenhalssituation zur Folge.

http://www.computerwoche.de/security/1932573/