

INTERVIEW

Nicolai Landzettel, Geschäftsführer von Data Sec UG, hat sich darauf spezialisiert, kleine und mittelständische Unternehmen im Bereich IT-Sicherheit zu beraten. Im Gespräch mit FACTS erläutert Landzettel typische Schwachpunkte und gibt Hilfestellungen für die Praxis.



NICOLAI LANDZETTEL, Geschäftsführer der Data Sec UG

FACTS: Laut der Studie „2011 Global State of Information Security Survey“ von Pricewaterhouse Coopers haben sich die meisten Unternehmen für dieses Jahr vorgenommen, ihre Investitionen in IT-Sicherheit zu erhöhen. In welchen Bereichen gibt es denn am meisten Nachholbedarf?

Nicolai Landzettel: Nach unserer Einschätzung sehen wir – vor allem bei mittelständisch geprägten Unternehmen – einen großen Bedarf im Bereich Gateway-Security. Ein noch dringlicherer Aspekt ist in den meisten Fällen allerdings zunächst die Erarbeitung und Umsetzung eines ganzheitlichen, durchdachten IT-Sicherheitskonzepts. Da gibt es noch eine ganze Menge Optimierungspotenzial.

FACTS: Doch die Verantwortlichen für IT-Sicherheit in mittelständischen Betrieben klagen häufig über knappe finanzielle und personelle Budgets, wenn es um das Thema IT-Sicherheit geht. Was empfehlen Sie als Experte?

Landzettel: Eigentlich haben mittelständische wie auch Enterprise-Unternehmen ganz ähnliche Anforderungen in puncto Sicherheit. Fast alle Unternehmen setzen heute Firewalls, Virenschutzlösungen und Ähnliches als punktuelle Lösungen ein. Wir erleben aber leider oft, dass sowohl externe IT-Betreuer als auch interne Verantwortliche es nicht schaffen, den Topentscheidern im Unternehmen die Wichtigkeit und Notwendigkeit eines durchgängigen Sicherheitskonzepts klar zu machen.

FACTS: Ein durchgängiges Sicherheitskonzept zu erarbeiten und durchzusetzen – wie funktioniert das?

Landzettel: In einem ersten Schritt fordern wir in einem Auditing eines Unternehmens die Vorstände und Geschäftsführer zu einer anschließenden Risikobewertung auf. Viele Geschäftsführer sind sich zwar durchaus der vorhandenen privaten Haftungsrisiken bewusst, doch macht es wenig Sinn, aus einem diffusen Schutzbedürfnis heraus ein Budget freizugeben, ohne zu wissen, vor was konkret man

sich eigentlich schützen will. Stellen Sie sich eine Flughafen-Sicherheitskontrolle vor, bei der die Sicherheitsmitarbeiter die Anweisung haben, alle Menschen durchzulassen. Dummerweise hat aber auch der schicke Metalldetektor gar keinen Strom. Ähnlich groteske Situationen treffen wir in den meisten Unternehmen an. Da finden Sie 0815-Firewalls ohne ein konzeptionell erarbeitetes, sinnvolles Regelwerk und oft auch ohne Support und regelmäßige Updates. Das ist natürlich völlig unzureichend. Eine Firewall muss mit Updates auf einem sicheren Stand gehalten werden und ohne vorherige Konzeption bringt sie dem Unternehmen praktisch nichts, sondern verursacht einzig und allein Kosten.

FACTS: Laut Einschätzung von IDC wird das Thema Mobile Security künftig noch wichtiger werden. Technikrends wie Unified Communications und eine stetig wachsende Anzahl „mobiler Mitarbeiter“ unterstützen diese Entwicklung zusätzlich. Was ist hinsichtlich dieser Entwicklung zu tun?

Landzettel: Ohne Frage erhöht sich das Gefährdungspotenzial für Unternehmen. Zum einen durch mobile Mitarbeiter, die unkontrolliert aus Fremdnetzen oder gar von öffentlichen Computern aus sensible Daten des Unternehmens zugreifen. Zum anderen haben Firmen keine Lösung, die das absichtliche oder unbeabsichtigte Kopieren vertraulicher Daten verhindert und die Daten der immer mobiler werdenden Mitarbeiter schützt – beispielsweise bei einem Diebstahl. Ein solides Sicherheitskonzept berücksichtigt aber auch diese Punkte umfassend.

FACTS: Web-2.0-Angebote und soziale Netzwerke wie Facebook, Twitter und Co. sind IT-Verantwortlichen häufig ein Dorn im Auge. Welche Vorkehrungen müssen getroffen werden, um mögliche Schäden zu vermeiden und Risiken zuverlässig auszuschließen?

Landzettel: Die meisten Verantwortlichen sehen diese Webangebote in erster Linie als Produktivitätskiller. Bevor konkrete Sicherheitsmaßnahmen ergriffen werden, müssen zunächst einige Fragen geklärt werden: Ist beispielsweise eine private Nutzung von Internet und E-Mail während der Arbeitszeit erlaubt? Wird ein Verbot durch Stichproben kontrolliert? Aus diesen Rahmenbedingungen ergeben sich verschiedenste Ausgangssituationen, die dann zum Beispiel ein Loggen oder Eingreifen in den Internetverkehr ausschließen oder eben ermöglichen. Es gibt aber auch „softere“ Handlungsmöglichkeiten, die weniger restriktiv wirken und dennoch den gewünschten Effekt erzielen.

FACTS: Was empfehlen Sie ganz konkret?

Landzettel: Eine Empfehlung wäre zum Beispiel, die Internetbandbreite für solche Produktivitätskiller auf die gute alte Modemgeschwindigkeit auszubremsen. Somit ist gewährleistet, dass die businesskritischen Anwendungen mit voller Bandbreite laufen. YouTube und Co. verlieren dagegen schnell ihre Attraktivität, denn wer wartet schon gern 15 Minuten auf den Start eines kurzen Videobeitrags. Daneben ist es extrem wichtig, die Mitarbeiter durch Informationen zu sensibilisieren und vor sich selbst zu schützen. Welcher Unternehmer findet schon gerne Fotos eines unpatentierten Prototypen bei Picasa oder Facebook?!