IT-SICHERHEIT

Walter Sedlacek, T–Systems: »Auch im Straßenverkehr ist normiert, dass das Auto regelmäßig zum Service muss.«

**Walter Sedlacek** ist Manager ESARIS Global Governance, Enhancement and Operations im Qualitätsbereich von T-Systems und Leiter des Arbeitskreises Security des Vereins »Zero Outage«. Er spricht über die Aufmerksamkeit für Sicherheit und eine dringend benötigte Normierung von Qualitäts- und Sicherheitsprozessen in Unternehmen.

VON MARTIN SZELGRAD

# »ES SOLLTEN NUR NOCH AUSREICHEND GEWARTETE PCS ANS NETZ GEHEN DÜRFEN«

**(+) PLUS:** Security wird in den meisten Unternehmen als wichtiges Thema erachtet, allerdings betrifft dies vor allem eine technische Ebene. Wie sieht Ihr Ansatz hier aus?

**Walter Sedlacek:** Gemeinsam mit einigen Firmen haben wir vor wenigen Jahren eine Art Landkarte entwickelt, wie IT-Sicherheit in Unternehmen aussehen sollte. Jeder hatte seine wichtigsten Themen eingebracht und aus den unterschiedlichen Perspektiven wurde ein umfassender Katalog erstellt: Client-Systeme, Server, Unternehmensprozesse und viele, viele andere Dinge – Technologie selbst macht hier gerade einmal 20 Prozent aus. Sich zu schützen ist die eine Sache – was aber macht man, wenn man bereits befallen ist? Es sind Fragen und Aufgaben für die Organisation, für eine effiziente Vorgehensweise und richtige Reaktionen im Falle, wenn tatsächlich einmal etwas passiert. Welche Prozesse sollten laufen? Welche Unternehmensteile, Partner und auch Kunden werden einbezogen? Welchen Ausbildungsgrad haben die Mitarbeiter? Alle dies muss ineinandergreifen.

**(+) PLUS:** Wie ist die Situation bei Unternehmen dazu in Österreich? Gibt es Sicherheitslücken, gibt es einen großen Aufholbedarf?

**Sedlacek:** Aus meiner Sicht gibt es Aufholbedarf. Man hat punktuell schon technisch gute Lösungen. Es gibt Firewalls und Virenschutz, gute Sicherheitskonzepte. Was es aber kaum gibt, ist eine Gesamtsicht auf das Thema – so wie es auch mit dem »Zero Outage«-Ansatz unternommen wird. Security wird hier aus allen Ecken beleuchtet, alle Abteilungen in Unternehmen sind involviert und arbeiten damit. Typischerweise finden Sie in Unternehmen Security-Abteilungen vor, in denen sich eine Handvoll Fachleute auf ihrem Gebiet perfekt auskennen. Die restlichen 7.000 Mitarbeiter haben von dem Thema aber keine Ahnung. Unsere Idee eines Security-Konzepts ist die inhärente Integration in alle Einheiten und Teile einer Organisation – das geht bis in den Einkauf, die Finanz und SAP-Abteilungen. Ein Beispiel: Die IT-Abteilung kann ihre Firewall bestmöglich konfigurieren. Das ist aber sinnlos, wenn die HR neue Leute einstellt, die einen eindeutigen Hacker-Hintergrund haben.

Wenn ein Sicherheitsvorfall passiert, ist es wichtig zu wissen, an welcher Stelle dies zuerst aufgetreten ist und wie schnell es sich verbreitet. Wird dies am Service-Desk korrekt bekannt gegeben und aufgenommen, kann auch richtig reagiert werden. Dieser Prozesse muss entsprechend implementiert werden, über alle Abteilungen hinweg, zentral organisiert. Ein verseuchter PC kann dann schnell und gezielt vom Netz genommen werden.

**(+) PLUS:** Es ist also nicht ausreichend, sich auf technische Vorkehrungen zu verlassen? Man muss sich auch auf die Aufmerksamkeit der Anwender verlassen können?

**Sedlacek:** Auf jeden Fall. Dazu müssen diese aber entsprechend trainiert und auch getestet werden – etwas, was auch wir regelmäßig in unserer Organisation tun. E-Mails, die auf verseuchte Internetseiten verlinken, kann man sich heutzutage in zehn Minuten erstellen. Die Baukästen dafür sind nicht schwer zu bekommen. Um hier bei Mitarbeitern eine »Awareness« für diese Gefahren im Tagesgeschäft des E-Mail-Verkehrs zu fördern, sind wiederholend Informationen wichtig. Die gilt für alle: vom Top-Management bis nach ganz unten.

**(+) PLUS:** Sollte man die Mitarbeiter hiermit nicht auch im Privaten abholen? Viele nutzen ihre privaten Geräte am Arbeitsplatz.

**Sedlacek:** Nun, hier kommt es einfach auf die Härtung der Systeme im Unternehmen an und inwieweit mit Privatgeräten überhaupt am Arbeitsplatz gearbeitet werden darf. Als Arbeitgeber hat man natürlich keinen Einfluss, was die Leute zuhause tun. Aber: Auch auf Endgeräten wie etwa einem iPhone können sensible Firmendaten mit einer Containerlösung verschlüsselt und gesichert werden – bei Geräteverlust lassen sich die Daten da auch aus der Ferne löschen. Technisch ist das keine große Herausforderung mehr, das bieten auch andere Dienstleister an. Die meisten Sicherheitsvorfälle passieren aber auch nicht aufgrund technischer Unzulänglichkeiten, sondern wegen prozessualer Fehler. Das kann ein Passwort auf einem Zettel neben dem Bildschirm sein, das jemand über eine gehackte Überwachungskamera ausliest – was tatsächlich bereits passiert ist. Angegriffen wird immer über das schwächste Glied, also sind ganzheitliche Sicherheitsmaßnahmen nötig.

So etwas gibt es in anderen Bereichen schon lange: Brandschutzgesetze behandeln das Thema Sicherheit über einzelne Ebenen hinaus. Bei IT-Sicherheit dagegen gibt es noch nicht einmal im Ansatz Gesetze oder Normen. Letztere wollen wir mit dem Verein Zero Outage etablieren und auch Firmen dazu zertifizieren. Und wir wollen diesen Weg auch mit unserem Security-Framework ESARIS ebnen.

**(+) PLUS:** Was ist das Besondere an dieser Lösung?

**Sedlacek:** Zum einen ist ESARIS keine IT-Lösung, sondern ein Konzept, eine Sicherheitsarchitektur. Sie kommt in Unternehmen ab 2000 Mitarbeitern zum Einsatz und unterstützt besonders auch die Arbeitsteilung in Firmen. Gerade bei globalen Wertschöpfungsketten muss Security standardisiert werden – damit alle vom Gleichen reden. Das Regelwerk muss aber auch in kleine Stücke für die unterschiedlichen Rollen in den Unternehmen teilbar sein. Ein Netzwerk-Administrator sieht damit einfach seine für ihn relevanten Teile – die trotzdem ineinandergreifen – und muss keine 500-Seiten-Normenschrift lesen. Ein weiterer entscheidender Faktor ist das Einbeziehen der Dienstleistungsebene des IT-Outsourcings, ein Bereich, in dem wir ja auch tätig sind. Die großen Frameworks gehen nicht genügend auf diesen Servicelevel in der IT ein, ESARIS tut dies sehr wohl.

**(+) PLUS:** Sie sprechen hier vor allem die Beziehung eines IT-Dienstleisters zum Unternehmenskunden an?

**Sedlacek:** Ja – das fängt schon beim Begriff des »Kunden« an, den Sie in keiner ISO-Norm finden werden.

**(+) PLUS:** Das heißt: Ein Sicherheitskonzept, das über die eigenen Grenzen einer Infrastruktur hinausgeht, braucht auch die Mitarbeit des Unternehmenskunden.

**Sedlacek:** In einem ersten Schritt braucht es die Akzeptanz beim Kunden, in einem zweiten Schritt die Mitarbeit. Im klassischen IT-Outsourcing wird der Kunde erst involviert, wenn es bereits brennt. In ESARIS sind regelmäßige Meetings vorgegeben, in denen mögliche Schwachstellen und wunde Punkte proaktiv diskutiert werden. Es ist wie beim Betrieb eines Fahrzeuges: Normiert ist, dass das Auto regelmäßig in die Werkstatt zum Service muss. Wer das nicht macht, darf nicht mehr fahren. Ich würde mir wünschen, dass analog ebenfalls nur ausreichend gewartete PCs ans Netz gehen dürfen.

**(+) PLUS:** Wer setzt ESARIS bereits ein?

**Sedlacek:** Kundennamen darf ich – typisch für die Sicherheitsbranche – nicht nennen. Was ich sagen kann: Es sind große Unternehmen aus Bereichen wie Oil & Gas und dem Bankenumfeld.

**(+) PLUS:** Wie aber können sich auch kleinere Unternehmen schützen? Gibt es etwas, wovon auch Firmen unter einer Größe von 2000 Mitarbeitern profitieren können?

**Sedlacek:** Wer möchte, kann hier auf eine Durchdeklination der Empfehlungen bis zum letzten Bit zugreifen. Nach oben hin wird es dagegen immer generischer. Der Abstraktionslevel ist frei wählbar und damit auch für KMU tauglich. Kleinere und mittlere Unternehmen gehen hier einfach nicht in die Detailtiefe, haben aber trotzdem das große Bild einer Sicherheitsarchitektur. Ein solcher Punkt in verschiedenen Detailgraden ist die Notwendigkeit eines Virenscanners auf jedem PC. Was die Software genau können muss, welche Heuristik angewendet wird – das muss in einem kleineren Rahmen nicht ausformuliert werden. Wichtig ist, dass es den Virenscanner überall gibt.

Natürlich wird das Risiko eines Schadensfalls geringer, wenn man sich an tiefergehende Empfehlungen hält. Das geht bis zum entsprechenden Config-File für den Cisco-Router oder Regeln für galvanische Trennung von Netzwerken in einem Rechenzentrum.

**(+) PLUS:** Wenn Sie nun eine einfache Empfehlung für die IT-Sicherheit in Unternehmen geben wollen – was wäre diese?

**Sedlacek:** Der wichtigste Sicherheitsfaktor ist immer noch der User. Dieser sollte im Umgang mit seinem PC über einen gewissen Hausverstand verfügen. Wachsam bleiben, skeptisch gegenüber unerwarteten Zuschriften und verdächtigen, tollen Versprechungen im Internet sein. Und bitteschön ein paar Euro in einen Virenschutz investieren. Mit einer gewissen Sensibilität ist schon viel gewonnen. ■

Foto: T-Systems