

InformationWeek

SCHLUSS MIT DEN

VON KURT BRAND* |
juergen.hoefling@informationweek.de

ANGST-SZENARIEN

Mit Panikmache lässt sich der mittelständische Entscheider nur selten von notwendigen Maßnahmen zur IT-Sicherheit überzeugen. Mit Recht: Der Normalschaden heißt nämlich nicht Totalverlust, sondern besteht in vergeudeter Zeit und damit Gewinnausfällen.

Internet-Sicherheit ist ein Teilbereich der IT-Sicherheit. Um beide steht es schlecht im Mittelstand. Das berichten die einschlägigen Medien unisono schon seit Jahren, und das ist auch die Erfahrung der meisten in diesem Feld tätigen Berater. Zu wenig Zeit und Geld sowie fehlendes Know-how werden immer wieder als Begründung für diese Mängel genannt. Dabei macht letztlich das Know-how den größten Aufwandsposten aus, denn es muss ständig aktuell gehalten werden.

ANGST IST EIN SCHLECHTER RATGEBER

Dass es mit der Internet-Sicherheit im Mittelstand nicht besser bestellt ist, daran haben indes die Anbieter von Sicherheitsprodukten und -leistungen ein gerüttelt Maß Schuld. Gelingt es doch diesen Anbietern relativ selten, treffende und gleichzeitig verständliche Leistungsinformationen zu geben. So wird in einem Werbeprospekt eines renommierten TK-Dienstleisters ein »Angebotspaket für optimale Internet-Sicherheit« zum Beispiel mit folgenden Begriffen umschrieben: Sicherheitspaket, Sicherheitslösung, Sicherheitssystem und Sicherheitskonzept. Dass es sich bei dem beworbenen Produkt um eine Firewall zum Schutz gegen Hacker handelt, wird jedoch nicht gesagt. Eine solche Firewall bietet freilich für sich alleine nicht diese »optimale Internet-Sicherheit«, wie im Werbeprospekt behauptet wird. Kein Wunder, dass die Internet-Sicherheit besonders im Mittelstand Schwachstellen hat. Mit Panikmache aber lässt sich der mittelständische

Entscheider nur selten auf den Weg der Besserung bringen. Denn der Normalschaden ist nicht der Verlust des Unternehmens, sondern die verlorene Zeit des Unternehmers und seiner Mitarbeiter.

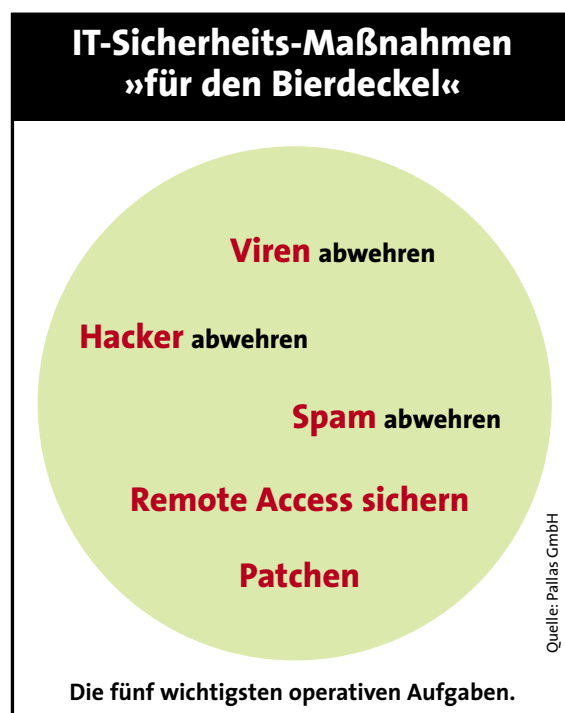
Viele Kunden zögern deshalb, von Angeboten der oben beschriebenen Art Gebrauch zu machen. Angesichts von Kundenzurückhaltung spielen die Anbieter dann häufig die »Angstkarte« aus. Einem mittelständischen Geschäftsführer den möglichen Untergang seines Unternehmens als Bedrohungsszenario anzubieten, ist aber für die Verbesserung

der Internet-Sicherheit nicht zielführend. Als Unternehmer ist er ohnehin gewohnt, Grenzkosten zu tragen. Er ist ja kein Angestellter eines Großunternehmens, der bestrebt sein muss, Risiken per Entscheidungsvorlage nach oben abzugeben. Horrorszenarien sind aber so weit vom Tagesgeschäft eines Mittelständlers entfernt, dass sie keine didaktische Wirkung erzielen können.

Überdies ist Angst bekanntlich ein schlechter Ratgeber. Der Kunde durchschaut die reißerische Darstellung und wird erst recht davon abgehalten, etwas für die Sicherheit zu tun. Ähnlich wenig Wirkung zeigt der Hinweis auf die Haftung des Geschäftsführers nach § 43 GmbH-Gesetz und die Strafandrohung bei Verletzung der Vermögensbetreuungspflicht.

VERGEUDETE ZEIT ALS HAUPTSCHADEN

Ein seriöser Sicherheitsdienstleister versucht nicht, seinen Kunden Angst zu machen, sondern schafft ein Klima des Vertrauens. Zwei Beispiele aus der Praxis sollen erläutern, womit der Mittelständler zu rechnen hat. Beispiel 1: Einem Unternehmen aus dem Kölner Raum mit etwa 60 Mitarbeitern wurde vor einigen Jahren die Personaldatei entwendet. Kurze Zeit spä-



ter erfolgte ein Abgang von Leistungsträgern, die mit punktgenauen Angeboten weggelockt werden konnten. Diesen Aderlass hat das Unternehmen nicht überstanden, es verschwand vom Markt. Ein solches Szenario wird indes einen mittelständischen Unternehmer kaum dazu bewegen, seine IT-Risiken deutlich zu senken. Er weiß, dass es sich hier um ein Restrisiko mit geringer Eintrittswahrscheinlichkeit handelt. Er kann sich letztlich auch nicht vor kriminellen Innetätern schützen, die in einem Vertrauensverhältnis stehen.

Der zweite Fall beschreibt die Situation eines typischen Mittelständlers deutlich besser. Ein Geschäftsführer eines etwa zehnköpfigen Unternehmens hatte sich 2004 das Sasser-Virus eingefangen. Das Virus fährt zunächst den Rechner herunter, der Geschäftsführer kann es aber mit einem geeigneten Entfernungstool von der Festplatte wieder löschen. Ihm ist auch bekannt, dass sich Sasser durch eine Lücke im Windows-Betriebssystem ver-

KURZ GEFASST

DIE WICHTIGSTEN ASPEKTE BEIM IT-SICHERHEITS-GRUNDSCHUTZ

- Der Normalschaden heißt nicht Totalverlust des Unternehmens, sondern bedeutet vergeudete Zeit.
- Vergeudete Zeit kann sehr schnell zu 30 Prozent Gewinn-Minderung führen.
- Mittelständler sollten mit Maßnahmen gegen Kernbedrohungen beginnen, die aber miteinander verzahnt sein müssen.
- Ein Sicherheits-Audit übersteigt oft die Möglichkeiten des Mittelstands,

die wichtigsten Bedrohungen können mittels Schwachstellenanalyse ermittelt und abgestellt werden.

- Mittelständler sollten Anbieter meiden, die mit Horrorszenarien auf Kundenfänger gehen.
- IT-Sicherheit als Dienstleistung sollte schon aus Know-how-Gründen in Erwägung gezogen werden, gleichwohl muss Grundwissen im Bereich IT-Sicherheit direkt im Unternehmen verbleiben.

ausgelöst wird. Natürlich drohen weitere Schäden, insbesondere bei Berufsgruppen, die aufgrund der Sensibilität der verarbeiteten Daten ein höheres Risiko tragen, wie zum Beispiel Ärzte und Steuerberater. Aber auch dort wird Zeitverlust der Primärschaden sein, dem dann weitere Negative Auswirkungen folgen können.

winn. 50 Stunden zusätzlicher Spam-Ausfall vernichten also mehr als 30 Prozent des Gewinns, wenn nicht an anderer Stelle die Produktivität gesteigert werden kann. Das entspricht einer Schadenssumme von mehr als 3000 Euro pro Mitarbeiter, wenn man 100 000 Euro Jahreskosten (Personal- und Nebenkosten) annimmt. Dieser Schaden muss nicht hingenommen werden, denn schon für 1 Prozent der Schadenssumme ist professioneller Spam-Schutz erhältlich, der 90 Prozent des einkommenden Spam-Verkehrs ausfiltert und – falls gewünscht – löscht.

SERIÖSE SICHERHEITSDIENSTLEISTER SETZEN NICHT AUF HORRORSZENARIEN.

breitet und dass man diese Lücke durch ein Sicherheitsupdate, einen so genannten Patch, schließen muss. Er fährt seinen Rechner nach Reinigung also wieder hoch, schließt ihn an das Internet an und beginnt von den Microsoft-Webseiten das Sicherheits-Patch herunter zu laden. Dies dauert ein paar Minuten, und das reicht dem Virus, um erneut zuzuschlagen. Sasser ist nämlich ein Netzwerk-Virus, das keine Email-Kommunikation für seine Verbreitung benötigt, sondern ein ungeschützt mit dem Internet verbundenes System direkt befällt. Das Sasser-Virus fährt den Rechner also wieder herunter, und das Spiel beginnt von neuem. Nach einigen weiteren Versuchen besorgt sich der Geschäftsführer das Patch auf anderem Wege und wird den Schädling so wieder los.

Der Schaden, der hier aufgetreten ist, beschränkt sich auf einen Zeit- und damit Effizienzverlust. Dies ist in aller Regel der Normalschaden, der durch Schwächen bei der Internet-Sicherheit

30 PROZENT GEWINNAUSFALL

Da der Zeitverlust im Mittelstand meist nicht erfasst und schon gar nicht finanziell bewertet wird, macht sich auch kein großes Schadensgefühl breit. »Et hätt noch immer jot jejanje«, wie es in Köln heißt. Das ist in Großunternehmen anders, wo jede Stunde in die Kostenträgerrechnung einfließt und solche Schäden/Kosten am Monatsende automatisch im Berichtswesen auffallen.

Dass Zeitverlust in jedem Unternehmen schnell den Gewinn aufzehrt, macht folgende einfache Überlegung klar. Wenn jeder Mitarbeiter täglich 15 Minuten für das Aussortieren und Wegwerfen von Spam-Mails verbraucht, summiert sich das auf 50 Stunden Zeitverlust jährlich und für jeden Mitarbeiter bei den üblichen 200 Tagen, die ein Arbeitnehmer pro Jahr produktiv sein kann. Erwirtschaftet das Unternehmen eine Rendite von 10 Prozent, bedeutet das: Von den geleisteten 1600 Jahresstunden erbringen nur 160 Stunden (= 10 Prozent) den Ge-

KONZENTRATION AUF KERNBEDROHUNGEN

Als mittelstandstauglicher Einstieg in den Verbesserungsprozess hat sich die Schwachstellenanalyse bewährt. Durch die Konzentration auf Kernbedrohungen und kritische Systeme können die Kosten erstaunlich niedrig gehalten werden. Außerdem bietet das Verfahren bei der Kosten-Nutzen-Relation die besten Werte. Dies verwundert nicht, denn ein Sicherheitszuwachs auf hohem Niveau kommt immer viel teurer als ein solcher am Anfang der Prozess-Kette.

Damit es mit der Internet-Sicherheit auch im Mittelstand vorangeht, ist in erster Linie ein Umdenken auf Anbieterseite erforderlich. Die Angebote sollten Maßnahmen gegen die wichtigsten Bedrohungen miteinander verzahnen. Einzelkomponenten führen in der Regel ebenso wenig zum Ziel wie Horrorszenarien. Und nicht zuletzt sollten bei der Leistungsinformation die Schutzfunktionen im Vordergrund stehen und nicht technische Details.

* DR. KURT BRAND ist Geschäftsführer des Beratungsunternehmens Pallas GmbH