

Virus Protection gegen Immunschwäche der IT-Landschaft

Von Jens Verstaen, freier Journalist in München

Obwohl die Ergebnisse einer aktuellen Studie der Meta Group zur IT-Sicherheit in Deutschland auf eine hohe Sensibilisierung für einzelne Security-Themen hinweisen, so stellte die Marktforschung bei der Umsetzung konkreter Maßnahmen noch erhebliche Mängel fest. In der Untersuchung erhalten 40 Prozent der Firmen beim Thema "IT-Security" gar das Prädikat "Hasardeure" – nicht nur angesichts neuer Computerbazillen wie Sobig-F ein beunruhigendes Ergebnis. Managed Security Service Provider wie Siemens Business Services helfen mit Virus Protection Services vor und bei elektronischem Schädlingsbefall und sorgen mit umfangreichen Security-Dienstleistungen für optimale IT-Sicherheit.

Die Relevanz von IT-Sicherheit ist unbestritten. Immerhin berichten 76 Prozent der deutschen Firmen von Schäden, die in den vergangenen zwei Jahren im eigenen oder bei ihnen bekannten Unternehmen entstanden waren. Doch viele Anwender orientieren sich nach Aussage der Meta Group bei Investitionen in IT-Sicherheit primär an rechtlichen Rahmenbedingungen, Anforderungen von Partnern und Kunden sowie an vergangenen Sicherheitsproblemen im eigenen Unternehmen. Dieses reaktive Investitionsverhalten birgt die Gefahr, dass viele neue Sicherheitslücken erst spät oder gar nicht gestopft werden.

Die Studie zeigt, dass entsprechende Maßnahmen in Deutschland bei etwa 70 Prozent der befragten Unternehmen ohne ganzheitlichen Blick und zu technologieorientiert betrachtet werden. Die Analysten schätzen dabei rund 30 Prozent der Unternehmen als "Techies" ein, die zwar durchaus vorbeugend, aber primär technologieorientiert investieren. 40 Prozent werden sogar als "Hasardeure" beurteilt, die aufgrund externer Anforderungen punktuelle Maßnahmen einleiten, aber gleichzeitig auch sicherheitsrelevante Zwischenfälle in Kauf nehmen, bevor sie umfassendere Vorkehrungen treffen.

Vom Handlungsbedarf beim Thema Sicherheit kann auch Klaus Martin, Practice Manager Security bei Siemens Business Services Deutschland, berichten. "Bei den Kunden gibt es in Puncto Sicherheit viel zu tun. Allerdings benötigen die Unternehmen für die Umsetzung von umfassenden Sicherheitsmaßnahmen Mitarbeiter, die das notwendige Security-Know-how über alle Themenfelder hinweg besitzen und im Notfall rund um die Uhr schnell und effizient reagieren können." Unter Umständen ist hierfür auch zusätzliches Personal notwendig, das wegen der wechselnden Anforderungen und der sich dynamisch verändernden Bedrohungspotenziale kontinuierlich und aktiv weitergebildet werden muss – weit über das Maß anderer Tätigkeitsfelder hinaus.

Eine Alternative stellen für die Unternehmen hier die "Managed Security Services" von externen IT-Dienstleistern dar, die den Firmen eine Reihe von Vorteilen bringen. So profitieren die Unternehmen beispielsweise davon, wenn die geeigneten Fachkräfte oder das Fachwissen im Haus nicht verfügbar sind oder die Organisation nicht mit diesen extrem Know-how-intensiven Aufgaben außerhalb der Kernkompetenzen belastet werden soll. Zudem können Managed Security Services als Einzelleistung bezogen werden – ein eigenes Sicherheitszentrum oder Outsourcing-Abkommen sind dafür nicht nötig. Klaus

Martin: "Bereits mit wenig Aufwand kann beim Thema Sicherheit viel erreicht werden. Diese Tatsache berücksichtigen wir durch einen modularen Aufbau unserer Managed Security Services."

Größte Gefahr: Vireninfektion

Die befragten deutschen Unternehmen sehen laut der Meta Group-Studie die Gefahr durch Virenbefall und bösartigen "Codes" als eindeutig höchstes Sicherheitsrisiko. Wie ernsthaft die Folgen einer derartigen Infektion sein können, zeigt "Sobig-F". Der Computerwurm öffnet auf den befallenen Rechnern Ports zum Internet, installiert einen eigenen Mailserver und sendet unbemerkt verseuchte E-Mails an Empfänger aus dem Adressbuch. Bei einigen Unternehmen sind die E-Mail-Systeme kollabiert, die Mitarbeiter waren praktisch per elektronischer Post nicht mehr erreichbar.

Sobig-F ist nur ein Vertreter der in zahlreichen unterschiedlichen Ausprägungen existierenden Spezies Computervirus – die Bedrohungen für die Unternehmen sind mannigfaltig. Doch die Anwender sind der Gefahr nicht schutzlos ausgesetzt. Es existieren zahlreiche wirksame Tools, die derartigen Schädlingen den Garaus machen. Diese Vielzahl an Schutzprogrammen birgt aber auch ein Problem: Welche Lösung ist die richtige für das jeweilige Unternehmen? Klaus Martin: " Virus Protection, also Antivirus-Software und dedizierte Services, bilden eine effiziente Schutzgrundlage. Allerdings muss diese Dienstleistung auf die spezifischen Bedürfnisse des Unternehmens abgestimmt sein."

Das bestätigt auch eine aktuelle Studie der ICSA Labs. Denn die Schäden durch Virenattacken nehmen zu, obwohl inzwischen auch Virenschutz-Tools großflächig verwendet werden. Eine Befragung von 300 IT-Verantwortlichen aus Unternehmen und Behörden ergab, dass mehr als 90 Prozent der Unternehmen über 90 Prozent ihrer PCs mit Virenschutzprogrammen ausstatten. Bei rund 70 Prozent kommen sogar automatisierte Virenschutzprogramme zum Einsatz, welche die Schädlingsbekämpfung ebenso wie notwendige Updates automatisch vornehmen.

Entscheidend ist jedoch nicht nur die Auswahl geeigneter Software, sondern der Aufbau und Betrieb von Logistikprozessen, die auch im Notfall die Verteilung von Informationen und aktualisierten Programmen in den Firmennetzen gewährleisten.

ICSA Labs empfiehlt eine Schutzstrategie, die aus mehreren, sich gegenseitig ergänzenden Komponenten besteht und so für den bestmöglichen Schutz sorgt. Eine derartige Strategie verlangt umfassendes Know-how und ist in der Regel von den Unternehmen alleine nicht zu realisieren – fachliche Hilfe ist unabdingbar. "Hier bieten wir mit unseren Virus Protection Services kompetente Unterstützung. Wir verfügen über ein eigenes Virus Competence Center (VCC), das sich ausschließlich mit der Bekämpfung von Computerviren beschäftigt", erklärt Klaus Martin. Die Kunden profitieren dabei von der Herstellerunabhängigkeit der Siemens-Tochter, die mit führenden Lösungsanbietern zusammenarbeitet und somit Best-Practice-Lösungen anbietet.

Die Services des IT-Dienstleisters umfassen bei Virus Protection (VP) nicht nur die Implementierung von entsprechenden Lösungen. Siemens Business Services

begleitet die Unternehmen mit einem modularen Dienstleistungsangebot von der Beratung über den Betrieb der kompletten Lösung bis hin zum Meldesystem und Support:

- *VP Audit*
Die Experten erstellen eine Bewertung der Ist-Situation nach internen Standards, entwerfen ein grobes Betriebskonzept unter Berücksichtigung der technischen Gegebenheiten und erarbeiten gemeinsam mit dem Unternehmen eine abstrakte Sicherheitsstrategie.
- *VP Pilot Support*
Um die Wirksamkeit des Konzeptes zu überprüfen, sollte das eingesetzte Produkt für einen begrenzten Zeitraum in einem kleineren Umfeld getestet werden. Zur Pilotierung erstellt das Virus Competence Center ein Konzept nach den Vorgaben des Unternehmens und unterstützt es mit einem temporären 3rd Level Support.
- *VP Rollout Planung*
Gemeinsam mit dem Kunden erarbeitet das Virus Competence Center einen Maßnahmenplan und eine Aufwandsschätzung als Basis für einen erfolgreichen Rollout und den laufenden Betrieb.
- *VP Rollout Support*
Der Rollout Support beinhaltet die technische Vorbereitung, Schulungen, Helpdesk bis zum Regelbetrieb des Virus-Protection-Konzeptes.
- *VP Support*
Nach der erfolgreichen Implementierung übernimmt Siemens Business Services den Regelbetrieb der Lösung. Zudem steht das Virus Competence Center dem Unternehmen bei Problemen rund um die Uhr an 365 Tagen im Jahr zur Verfügung. Durch einen Antivirus-Radar und ein Warnsystem werden neue Virenbedrohungen schnell erkannt und eingetretene Virenangriffe durch Incident Handling gemeistert.

"Ziel unserer Services ist ein Schutz der IT-Systeme mit allen Applikationen, Daten und Internet-Diensten, damit sich die Unternehmen ungestört auf ihre Kernaufgaben konzentrieren können", erklärt Klaus Martin. Denn in der Computerwelt ist es wie im normalen Leben: Die Bedrohungen durch Viren müssen ernst genommen und mit fachmännischer Hilfe bekämpft werden.