



KMU-Studie von Sophos:

Sicherheit auf dem Schirm

Mitarbeiter in KMU zeigen zunehmend Bewusstsein für Cybergefahren und IT-Sicherheit

Wiesbaden, 12. Mai 2015 Sicherheitsunternehmen mahnen seit Jahren, spektakuläre Medienberichte über Cyberattacken und Datenklau bei großen Unternehmen tun ihr Übriges: Cyberkriminalität und IT-Sicherheit scheinen keine Nischen-Themen für Fachpublikum mehr zu sein, sondern auch im Bewusstsein einer breiten Öffentlichkeit angekommen. Wie stellt sich die Situation in KMU bei deren Mitarbeitern dar? Eine Studie von Sophos und techconsult hat dies untersucht.

Immer wieder ließen sich in der Vergangenheit menschliche Fehler als Ursachen für IT-Sicherheitsvorfälle in Unternehmen identifizieren: Mitarbeiter, die unachtsam oder ungeschult waren im Umgang mit Datensicherheit. Hier bestand Handlungsbedarf für Unternehmen.

Die Studie von Sophos zeigt, dass sich eine positiv stimmende Entwicklung vollzogen hat was das Bewusstsein von Mitarbeitern in KMU für Cybergefahren und die Notwendigkeit von IT-Sicherheitsmaßnahmen angeht. So vermeldeten im Rahmen der Befragung immerhin rund 66 Prozent der Unternehmen, dass ihre Mitarbeiter in den vergangenen Jahren sowohl sensibler für das Thema Datensicherheit als auch zuverlässiger im Einhalten der entsprechenden Unternehmensrichtlinien geworden seien. Etwas mehr als die Hälfte der Unternehmen konnte zudem feststellen, dass die Mitarbeiter das Thema IT-Sicherheit häufiger als früher von sich aus thematisieren.

Schulungen, Poster, Honeypots

Auch die Unternehmen selbst tun etwas, um den Faktor Mensch als Fehlerquelle so klein wie möglich zu halten. Schulungen sind hierbei offensichtlich das Mittel der Wahl. Gut 65 Prozent der Unternehmen gaben an, ihre Mitarbeiter regelmäßig hinsichtlich der möglichen Gefahren durch Cyberkriminalität zu schulen. Aber auch Plakatives ist beliebt: 54 Prozent der Unternehmen weisen der Studie zufolge ihre Mitarbeiter per Poster oder E-Mail-Newsletter auf mögliche Gefahren hin. Und 11 Prozent der Unternehmen gehen noch einen plakativen Schritt weiter und starten sogar Honeypot¹-Aktionen, um den Mitarbeitern die Gefahren zu veranschaulichen. Hierbei werden gezielt gesicherte Umgebungen als Fallen für Hacker eingerichtet, um zu sehen wie Angreifer vorgehen und welcher Art die Angriffe sind. Nur wenige Unternehmen, 6,7 Prozent, setzen auf Mitarbeitergespräche zum Thema IT-Sicherheit und noch weniger, nämlich nur gut 3 Prozent, fahren interne Awareness-Kampagnen für den Schutz der Unternehmensdaten.

¹ „Als *Honeypot* (oder früher auch *Iron Box*) wird in der [Computersicherheit](#) ein [Computerprogramm](#) oder ein [Server](#) bezeichnet, der die [Netzwerkdienste](#) eines Computers, eines ganzen [Rechnernetzes](#) oder das Verhalten eines Anwenders simuliert. Honeypots werden eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Erfolgt ein Zugriff auf einen derartigen virtuellen Dienst oder Nutzer, werden alle damit verbundenen Aktionen protokolliert und gegebenenfalls ein Alarm ausgelöst. Das wertvolle reale Netzwerk bleibt von Angriffsversuchen möglichst verschont, da es besser gesichert ist als der Honeypot.“ *Quelle: Wikipedia*

Datendiebstahl, Cloud-Server, Schusseligkeit: Die großen Ängste

Was die Bedrohungsszenarien angeht, so zeigt sich, dass alle Unternehmen zu jeweils gleichen Teilen in vier Bereichen eine mittelgroße Bedrohung für Unternehmen sehen. Interessant ist dabei, dass zwei Szenarien Bedrohungen von außen darstellen und zwei Szenarien mögliche interne Schwachstellen beschreiben.

Auf die Agenda der Bedrohungen von extern haben die Unternehmen zum einen den Diebstahl personenbezogener oder produktionstechnischer Daten (etwa Passwörter, Adressen etc.) durch Cyberkriminelle gesetzt. Zum anderen besorgt die Unternehmen ein möglicher Verlust von Daten durch deren Speicherung auf externen Cloud-Diensten. Hier bestätigt sich einmal mehr das anhaltende Misstrauen gegenüber Cloud-Services bei KMU im deutschsprachigen Raum.

Misstrauen besteht aber offenkundig auch gegenüber den eigenen Mitarbeitern. Zwei Bereiche haben die Unternehmen hier als Bedrohungsszenarien identifiziert: Man fürchtet einerseits die Schusseligkeit von Mitarbeitern in Form von verlorenen Daten auf verlorenen Geräten. Andererseits erwägt man aber auch die Möglichkeit der Absicht. Die Gefahr, dass Mitarbeiter z.B. auf USB-Sticks o.ä. Daten stehlen könnten bewerten die Unternehmen als ebenso hoch wie die übrigen genannten Bedrohungsszenarien.

Über die Studie

Für die Studie, die unter anderem Aspekte wie Handhabung und Zugriff auf Unternehmensdaten, den Einsatz von Sicherheitsprodukten oder eben das Sicherheitsbewusstsein der Mitarbeiter beleuchtet wurden 305 Unternehmen der unterschiedlichsten Branchen wie Industrie, Dienstleistungen oder Telekommunikation in Deutschland, Österreich und der Schweiz befragt.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos

Jörg Schindler, PR Manager CEEMEA

joerg.schindler@sophos.com, +49-721-25516-263

TC Communications

Arno Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Christiane Capps, +49-174-3335550

Ulrike Masztalerz, +49-30-55248198

sophos@tc-communications.de