KMU-Studie von Sophos:

Sicherheit auf dem Schirm

Bewusstsein für IT-Sicherheit steigt sowohl bei KMU als auch bei den Mitarbeitern

Wien, 9. Juni 2015 Cyberkriminalität und IT-Sicherheit sind keine Insider-Themen mehr sondern bei Medien und Menschen grundsätzlich angekommen. Zu häufig sind die Vorfälle bei großen Unternehmen, bei Behörden, Medienhäusern etc., zu präsent die Berichterstattung darüber. Auch in kleinen und mittelständischen Unternehmen in Österreich, Deutschland und der Schweiz ist IT-Sicherheit als Thema mehr in den Fokus gerückt. Zu diesem Ergebnis kommt eine von Sophos und techconsult. 305 Unternehmen aus Deutschland, Österreich und der Schweiz und aus unterschiedlichsten Branchen standen dafür Rede und Antwort.

Gesteigertes Sicherheitsbewusstsein bei den Mitarbeitern
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 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
Die Unternehmen selbst tun einiges, 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-Mai-Newsletter auf mögliche Gefahren hin. Und 11 Prozent der Unternehmen gehen noch einen plakativen Schritt weiter und starten sogar Honeypot[1]-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.

Software Equipment von einem Hersteller, einfach in der Handhabung
Auch die Unternehmen scheinen sich mit dem Thema IT-Sicherheit zunehmend intensiv zu beschäftigen. So zeigt sich in der Studie, dass Unternehmen heute ihre Anforderungen an

---

[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*

Sicherheitslösungen recht klar benennen können. Eine leichte Handhabung, einfaches Ausrollen neuer Policies auf verschiedene Plattformen und Geräte, die Kommunikation einzelner Module untereinander, ein zentrales Management, keine Performance-Einbußen sowie umfassender und schneller Support waren die Aspekte, die am häufigsten genannt und jeweils auch für ähnlich wichtig bewertet wurden. Lediglich ein Aspekt erwies sich als noch relevanter – die Fokussierung auf einen bis maximal zwei Hersteller. Bereits jetzt setzen zahlreiche Unternehmen dies um: So gaben 40,7 Prozent der befragten Unternehmen an, Software von einem einzigen Hersteller im Einsatz zu haben, 50,5 Prozent Prozent nutzen die Lösungen von zwei Herstellern.

Viel Endpoint, wenig Dateiverschlüsselung
Was den tatsächlichen Einsatz von software angeht, kommt die Studie zu folgenden Ergebnissen: Unternehmen schützen besonders Endpoint Geräte. Gut 80 Prozent der befragten Unternehmen gaben an, hier Sicherheitssoftware einzusetzen. Mobile-Security-Produktehaben hingegen nur noch knapp 47 Prozent im Einsatz, Datenverschlüsselung gibt es in 45 Prozent der Unternehmen, Datei-oder Ordnerverschlüsselung ist ebenso wie ein Mobile-Device-Management System jeweils nur bei gut 36 Prozent der befragten Unternehmen im Einsatz. Hier besteht Luft nach oben.

Datendiebstahl, Cloud-Server, Trotteligkeit: Die großen Ängste
Auf die Agenda der Bedrohungen 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 Mitarbeiten 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 das Sicherheitsbewusstsein der Mitarbeiter beleuchtet wurden 305 Unternehmen der unterschiedlichsten Branchen wie Industrie, Dienstleistungen oder Telekommunikation in Österreich, Deutschland 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 Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de