# Malware, Menschen, Phishing

## Dies sind die Top 3 der aktuellen Sicherheitsgefahren für Unternehmen so die aktuelle Next Gen Endpoit Security Studie von IDC

**Wiesbaden, 12. Juli 2017 –** Passwörter auf der Schreibtischunterlage notieren, Viren-verseuchte Anhänge öffnen oder einfach mal die Tastatur mit Kaffee fluten – Mitarbeiter können einem Unternehmen ganz schön zusetzen. Sophos hat sich erneut an der aktuellen Multi-Client-Studie der IDC zum Thema Next Gen Endpoint in Deutschland beteiligt. Und die stellt klar: Die drei größten Sicherheitsrisiken im Unternehmen bleiben Malware, unbeabsichtigtes Fehlverhalten von Anwendern und Phishing-Attacken.

**Gold für Malware, Silber für fehlerhaftes Mitarbeiterverhalten und Bronze für Phishing**
Die IT-Sicht auf die aktuellen Sicherheitsrisiken ist deutlich: Auf Platz 1 steht mit einer Nennquote von 53 Prozent Malware, wie Viren, Trojaner, Würmer, Spy- und Ransomware. Die Silbermedaille (41 Prozent) geht an unbeabsichtigtes Fehlverhalten von Anwendern. Drittplatzierter mit 39 Prozent sind Phishing und Social Engineering, also simpel gesagt: das Durchwühlen des Papierkorbs nach Passwörtern etc.

Business Entscheider halten mit 64 Prozent Phishing-Attacken sogar für das größte Sicherheitsrisiko im Unternehmen. Doch auch der Mitarbeiter – sei es mit vorsätzlichem oder schlichtweg trotteligem Verhalten – genießt oftmals keinen guten Ruf, mit 44 Prozent Nennung gilt er als zweitgrößtes Sicherheitsrisiko. Diebstahl von Daten (39 Prozent), versehentliches Versenden von Dokumenten (37 Prozent) aber auch der Diebstahl von Geräten (mit immerhin 26 Prozent Nennung an 10. von 16 Stellen) machen den Mitarbeiter zum Schädling – zumindest für die Sicherheit des Unternehmens.

**Mitarbeiter als Schädlinge? Schulungen helfen. IT-Security muss zur Routine werden.**
Insgesamt gehen im Durchschnitt ein Drittel aller Sicherheitsvorfälle auf Anwender zurück. Für Unternehmen bleibt der Mitarbeiter damit ein hohes Sicherheitsrisiko. Was tun? „Sensibilisieren, regelmäßig Schulen durch Workshops und vielleicht auch einmal die Komplexität der eigenen Sicherheitsregeln überdenken“, fasst Michael Veit, Security Experte bei Sophos, die Hausaufgaben für Unternehmen zusammen. „Absichtliches, schadhaftes Verhalten von Mitarbeitern lässt sich damit nicht gänzlich verhindern. Aber für alle anderen Mitarbeiter gilt es, bei ihnen eine Wahrnehmung und Akzeptanz für die Notwendigkeit von IT-Sicherheit und entsprechenden Verhaltensregeln und Software-Lösungen zu schaffen. IT-Security muss schlichtweg für alle zur Routine werden.“

**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
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de