



## Same procedure as every year

*Allen Trends und „Threat Predictions“ zum Trotz:  
Auch in 2017 werden 99 Prozent der IT-Sicherheitsvorfälle derselbe olle Kram wie  
immer sein.*

### Ein Kommentar von Chester Wisniewski, Senior Security Advisor bei Sophos

Immer gegen Ende eines alten oder zu Beginn eines neuen Jahres gibt es die Voraussagen, auch so genannten „Threat Predictions“, „Threat Reports“ oder „Threat Trends“ der Sicherheitssoftware-Unternehmen und anderer Experten zu den drohenden Gefahren im kommenden Jahr. Dies ist eine wichtige und notwendige Einschätzung von Spezialistenseite, die tatsächlich einen wichtigen Aufschluss darüber gibt, wohin sich die „Gegenseite“, also die Cyberkriminalität entwickelt. Das heißt, welche Schwerpunkte sie vermutlich setzt und womit sie womöglich auf neuem Wege Geld machen will. Natürlich wird auch Sophos wieder seine Einschätzung über die Cybergefahren für das nächste Jahr abgeben. Doch vieles, was da oftmals spektakulär angekündigt wird, hat oft wenig mit der Realität in Unternehmen zu tun.

Denn auf die Frage „Was ist die größte Cybergefahr im nächsten Jahr?“ gibt es nur eine – vielleicht aus journalistischer Sicht unbefriedigende aber eben wahrheitsgemäße – Antwort: Zu 99 Prozent besteht die Arbeit der IT-Sicherheit in Unternehmen aus daily business. Security-Anbieter, Journalisten und Experten bemühen natürlich gern die Angst vor dem drohenden möglichen Zero-Day-Angriff oder davor, dass Regierung XY sich in die Kommunikationsdaten unbescholtener Bürger eines anderen Landes hacken könnte. Die Wahrheit ist aber, dass die meisten Unternehmen es – wie immer – mit den alltäglichen Gefahren zu tun haben werden: mit Cyber-Gangstern, die Passwörter stehlen, mit ins Unternehmensnetz geschleuster erpresserischer Ransomware oder auch mit unzähligen Versuchen Menschen auf falsche Links zu locken.

Ich rate deshalb allen Unternehmen, sich vor allem auf die notwendige Basisarbeit in der IT-Sicherheit zu besinnen, um die täglichen Bedrohungen abzuwehren – am besten natürlich alle. Wer hierbei wirklich konsequent und Effizient vorgeht, der hat die nötige Zeit übrig, um sich auch mit Elite-Hackern, mit Regierungsspionen oder anderen spektakulären Cyber-Gefahren auseinanderzusetzen.

21. Dezember 2016

### 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](http://www.sophos.de).

**Pressekontakt:**

Sophos

Jörg Schindler, PR Manager CEEMEA

[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications

Arno Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

[sophos@tc-communications.de](mailto:sophos@tc-communications.de)