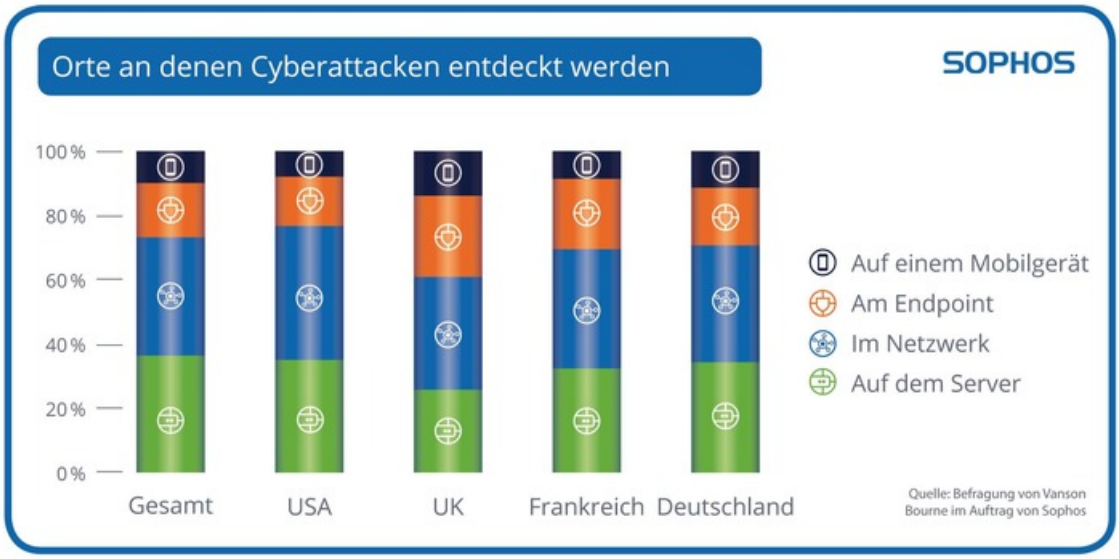
Sophos GmbH

07.03.2019 – 11:00 Uhr

Sophos Umfrage: Cyberkriminelle Aktivitäten werden meist auf Servern oder im Netzwerk entdeckt - Aufenthaltsdauer und erster Angriffspunkt sind oft unbekannt



Wiesbaden (ots) -

Wichtigste Umfrageergebnisse:

- Die meisten Aktivitäten von Cyberkriminellen werden aus internationaler Sicht auf Servern (37 Prozent) oder im Netzwerk (37 Prozent) entdeckt; 17 Prozent werden auf Endpunkten und nur knapp 10 Prozent auf mobilen Geräten gefunden.
- 28 Prozent der deutschen Unternehmen benötigen eine bis vier Stunden bis zur Erkennung von Cyberattacken im System, 37 Prozent zwischen vier und zwölf Stunden.
- Im internationalen Durchschnitt verbringen Unternehmen, die pro Monat einen oder mehrere potenzielle Sicherheitsvorfälle untersuchen, 48 Tage im Jahr mit forensischen Aufgaben.

Sophos stellt die Ergebnisse seiner globalen Umfrage vor, die bei über 3.100 IT-Entscheidungsträgern aus mittelständischen Unternehmen in 12 Ländern erfolgte, darunter die USA, Deutschland, Frankreich und Großbritannien. Die Auswertungen der internationalen Antworten zeigen, dass Unternehmen die größten Attacken von Cyberkriminellen hauptsächlich auf Servern (37 Prozent) und in Netzwerken (37 Prozent) entdecken. An den Endpoints werden nur 17 Prozent und auf mobilen Geräten lediglich 10 Prozent entdeckt. Die Umfrageergebnisse bei deutschen Unternehmen sind weitgehend deckungsgleich. Frankreich bestätigte für Endpoints 22 Prozent, Indien ist mit knapp 19 Prozent internationaler Spitzenreiter auf Mobilgeräten.

"IT-Manager sollten geschäftskritische Server und Netzwerke schützen und Angreifer davon abhalten, überhaupt in das IT-System einzudringen", so Michael Veit, IT-Security-Experte bei Sophos. "Neben dem Schutz der Server und Netzwerke muss der Fokus auch auf den Endpoint liegen, da die meisten Cyberangriffe dort beginnen. Eine höher als erwartete Anzahl von IT-Managern kann nach wie vor nicht sagen, wie die Angriffe in das System gelangen und wie lange sie sich bereits in der IT-Infrastruktur befinden."

Hohes Risiko durch mangelnde Transparenz in der IT-Security

20 Prozent aller international befragten IT-Manager, die im vergangenen Jahr einer oder mehrerer Cyberattacken ausgesetzt waren, können nicht genau bestimmen, wie die Angreifer in die Umgebung gelangt sind. In Deutschland bestätigten dies 21 Prozent der Befragten, in Brasilien sogar 26 Prozent. 17 Prozent wissen laut Umfrage nicht, wie lange die Gefahr bereits im Unternehmen war, bevor sie erkannt wurde. 16 Prozent waren in Deutschland der gleichen Meinung. Um die mangelhafte Transparenz zu mindern, benötigen IT-Manager eine EDR- Technologie (Endpoint Detection and Response). Damit können die Ausgangspunkte der Attacken und die digitalen Fußspuren der Angreifer durch ein Netzwerk aufgedeckt werden.

"Wenn IT-Manager den Ursprung beziehungsweise die Bewegung eines Angriffs im System nicht kennen, lässt sich weder das Risiko senken noch die Angriffskette unterbrechen, um eine weitere Infiltration zu verhindern", sagt Michael Veit. "EDR hilft Risiken zu identifizieren und ist ein integraler Bestandteil für die dringend benötigte Threat-Intelligence in Unternehmen."

Hohen forensischen Zeitaufwand mit EDR senken

Laut Umfrage verbringen Unternehmen, die monatlich einen oder mehrere potenzielle Sicherheitsvorfälle untersuchen,

durchschnittlich 48 Tage im Jahr (respektive vier Tage im Monat) mit der Untersuchung. Es überrascht nicht, dass deutsche IT-Manager die Identifizierung von verdächtigen Ereignissen (37 Prozent), das Alarmmanagement (13 Prozent) und die Priorisierung von verdächtigen Ereignissen (14 Prozent) als die drei wichtigsten Funktionen von EDR-Lösungen einstufen, um die Zeit für die Identifizierung und Reaktion auf Sicherheitswarnungen zu verkürzen.

"Die meisten einfacheren Cyberangriffe können innerhalb von Sekunden bereits an den Endpoints gestoppt werden, ohne einen größeren Alarm auszulösen. Hartnäckige Angreifer, die beispielsweise gezielte Ransomware wie SamSam verbreiten, nehmen sich die nötige Zeit, um ein System zu infiltrieren. Sie erraten schlecht gewählte Passwörter auf Systemen, die von außen zugänglich sind (RDP, VNC, VPN usw.). Fassen sie einmal Fuß, bewegen sie sich möglichst unauffällig durch das Netz, bis der Schaden angerichtet ist", sagte Veit. "Sobald Cyberkriminelle wissen, dass bestimmte Arten von Angriffen funktionieren, replizieren sie diese typischerweise im gesamten System. Wenn IT-Manager jedoch mit EDR eine intensive Verteidigung betreiben, können sie einen Vorfall schneller untersuchen und Infektionen im gesamten System finden. Gezieltes Aufdecken und Blockieren von Angriffsmustern reduzieren den Zeitaufwand, den IT-Manager mit der Untersuchung potenzieller Vorfälle verbringen."

57 Prozent aller Befragten (60 Prozent in Deutschland) gaben an, dass sie die Einführung einer EDR-Lösung planen. EDR hilft auch, eine Qualifikationslücke zu schließen. 80 Prozent der international befragten IT-Manager wünschen sich laut der Umfrage ein stärkeres Team, bei den deutschen Unternehmen sind es sogar 81 Prozentpunkte.

Umfrageergebnisse im Detail

Weitere Informationen stehen im Dokument "Sieben Unbequeme Wahrheiten der Endpoint Security" unter https://www.sophos.com/de-de/truths.aspx

Die "Sieben Unbequeme Wahrheiten der Endpoint Security"-Umfrage wurde von Vanson Bourne, einem unabhängigen Spezialisten für Marktforschung, von Dezember 2018 bis Januar 2019 durchgeführt. Die Umfrage erfolgte bei 3.100 IT-Entscheidungsträgern in 12 Ländern und auf sechs Kontinenten in den USA, Kanada, Mexiko, Kolumbien, Brasilien, Großbritannien, Frankreich, Deutschland, Australien, Japan, Indien und Südafrika. Alle Befragten sind aus Unternehmen mit 100 bis 5.000 Mitarbeitern.

Über Sophos

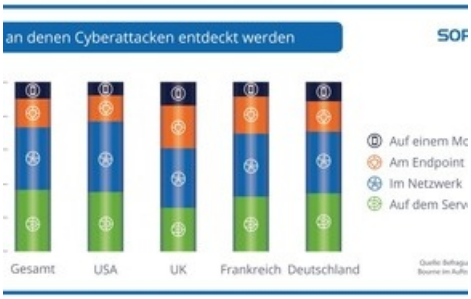
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security- Lösungen an, die 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.

Kontakt:

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

Medieninhalte



Orte an denen Cyberattacken entdeckt werden. Weiterer Text über ots und www.presseportal.de/nr/52556 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/Sophos GmbH"

Zeit bis Cyberattacken entdeckt werden. Weiterer Text über ots und www.presseportal.de/nr/52556 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/Sophos GmbH"