„Die Ergebnisse in der DACH-Region sind zwar enttäuschend, entsprechen aber dem, was wir in Nordamerika, Asien und anderen Regionen beobachten."

„Der Krieg in der Ukraine hat die Einstellungen nicht wirklich verändert."
Chester Wisniewski, Principal Research Scientist, Sophos

Umfrage in DACH zeigt: IT-Sicherheit ist keine Chefsache

Sophos stellt Unternehmensleitungen in Handel, Dienstleistung und verarbeitendem Gewerbe die Gretchenfrage:
Sag, Chef, wie hältst du´s mit der IT-Sicherheit?

- *Unterschiede nach Unternehmensgröße: Je größer das Unternehmen, desto weniger nah ist das Thema am CEO*
- *Unternehmensführungen wähnen sich in IT-Sicherheit*
- *Weltpolitische Lage hat wenig Einfluss auf die Bedeutung der IT-Sicherheit*
- *Zusatzkosten sind größte Sorge im Falle eines Sicherheitsvorfalls*

Es gibt zahlreiche gute Gründe, die Sicherheit der Daten in Unternehmen und Organisationen strategisch zur Chefsache zu erklären: Angefangen bei einer fortschreitenden Komplexität der Unternehmens-IT, Datenschutzregularien, Homeoffice, mobilem Arbeiten und Einbindung von IOT (Internet of Things) über prominente Cyberattacken auf Großunternehmen oder Einflussnahmen von Hackergruppen auf politische Entwicklungen bis hin zu spezialisierten Cyberangriffen auf kritische Infrastrukturen oder vulnerable Branchen wie das Gesundheitswesen. Dies sind einige willkürlich gewählte Beispiele, die Liste ist lang. Zunehmend wird ergo auch aus Fachkreisen gefordert, Schutz der Unternehmens-IT zum Managementthema zu machen.

Welche Bedeutung hat das Thema IT-Sicherheit aber tatsächlich ganz oben in den Chefetagen deutscher, österreichischer und Schweizer Unternehmen? Wie hoch schätzen die Unternehmensführungen die Gefahr cyberkrimineller Angriffe ein und welche Folgen für das operative Geschäft aufgrund von Hacker-Attacken erwarten sie am ehesten? Hat die aktuelle weltpolitische Lage einen Einfluss auf Wahrnehmung und Entscheidungen hinsichtlich der IT-Sicherheit?

Diese und eine Reihe weiterer Aspekte wollte das IT-Sicherheitsunternehmen Sophos in einer breit angelegten Studie herausfinden. Das Meinungsforschungsinstitut Ipsos hat hierfür im Frühsommer dieses Jahres hohe und höhere Führungskräfte (C-Level) in den drei Ländern befragt. IT-Personal wurde hierbei ausdrücklich ausgenommen.

Einige wichtige Erkenntnisse aus der Studie in der Übersicht:

- **IT-Sicherheit ist in Deutschland keine Chefsache.** Die IT-Abteilungen sind in der Verantwortung. Ein Drittel der Unternehmen setzt auf externe IT-Dienstleistungen.

- **Weltpolitische Lage und Krieg haben wenig Einfluss auf das Sicherheits-bewusstsein bei Managerinnen und Managern.** Nur ein Drittel sieht durch die aktuelle weltpolitische Lage den Blick für IT-Sicherheit nochmal geschärft.

- **Die Chefetagen wiegen sich bei IT-Sicherheit in Sicherheit.** Die Mehrheit gibt an, bereits seit längerem gut gewappnet zu sein.

- **C-Level-Verantwortliche erwarten insbesondere wirtschaftliche Folgen durch Cyberangriffe.** Wiederherstellungskosten oder Störungen der kaufmännischen Abläufe stehen im Fokus. Den Verlust von Kunden und Beschäftigten sowie mögliche Ausfälle im Rahmen der Lieferketten erwarten die wenigsten.

- **Unternehmen in Deutschland, Österreich und der Schweiz mit sehr ähnlichen Ergebnissen**

Höher aufgehängt und doch: IT-Sicherheit ist keine Chefsache. Die IT ist in der Pflicht.
Die große Mehrheit der befragten Manager (rund 81 Prozent) gibt an, ein hohes bis sehr hohes Bewusstsein für IT-Sicherheit zu haben. Auch wurde den Angaben aller Befragten zufolge in der Mehrheit der Unternehmen (über 60 Prozent) die IT-Sicherheit innerhalb der zurückliegenden drei Jahre auf eine höhere bzw. die höchste Hierarchieebene angesiedelt.

Hier offenbart sich ein interessanter Widerspruch, denn bei der Frage nach der tatsächlichen Verantwortung für die IT-Sicherheit zeigt sich dann doch ein anderes, durchaus zu erwartendes Bild: Je größer die Unternehmen sind, desto weniger steht die Führungsebene in der Verantwortung. Dies gilt vor allem für Unternehmen mit mehr als 200 Mitarbeitenden, hier geben nur 1,9 Prozent der Befragten an, dass die IT-Sicherheit auf Geschäftsführungs- bzw. Vorstandsebene angesiedelt ist. Bei kleineren Unternehmen mit bis zu 199 Mitarbeitenden sowie im Handel liegt dieser Wert deutlich höher, hier ist der Chef zu rund 22 Prozent noch höchstpersönlich mit eingebunden.

Die Hauptverantwortung für Cybersicherheit trägt in größeren Unternehmen zu 49,1 Prozent die eigene IT-Abteilung, bei 36,5 Prozent der kleineren Unternehmen sind ebenfalls die eigenen IT-Teams in der Pflicht. Mit 35,8 Prozent bei den größeren sowie 33,1 Prozent bei den kleineren Unternehmen überträgt zudem jeweils ein gutes Drittel aller Unternehmen die Verantwortung für ihre IT-Sicherheit auf externe Dienstleister.

Wenig Ukraine-Effekt: Deutsche Chefetagen wähnen sich in IT-Sicherheit
Selbstverständlich war es Sophos auch ein Anliegen zu erfahren, ob und inwieweit sich angesichts der weltpolitischen Lage und des aktuellen Kriegs in Europa, der bereits weit lange vor der eigentlichen militärischen Auseinandersetzung auf Cyberebene tobte, die Wahrnehmung und Bedeutung von IT-Sicherheit innerhalb der letzten zwei Jahre verändert haben. Hierzu bestätigten 23 Prozent der Befragten aus Unternehmen mit mehr als 200 Mitarbeitenden sowie knapp 36 Prozent aus kleineren Unternehmen, dass Cybersicherheit noch wichtiger geworden sei.

Mehrheitlich jedoch fühlt man sich offenbar ohnehin sehr sicher: 53 Prozent der kleineren und sogar knapp 70 Prozent der größeren Unternehmen geben an, dass sich hinsichtlich des Bewusstseins für das Thema Cybersicherheit in den letzten zwei Jahren nichts verändert habe und man hierfür bereits gut aufgestellt gewesen sei.
Auch in Bezug auf die bestehenden IT-Sicherheitsstrukturen im Unternehmen herrscht Zufriedenheit: 62,2 Prozent geben an, Ihr Unternehmen sei gut bis sehr gut gegen Cyberattacken gewappnet, bei den Entscheidern unter 45 Jahre liegt dieser Wert sogar noch um 2,5 Prozentpunkte höher.

Einen cyberkriminellen Angriff auf ihr Unternehmen halten gut 58 Prozent für wahrscheinlich bis sehr wahrscheinlich, knapp 39 Prozent betrachten diesen Fall als eher unwahrscheinlich.

Cyberattacken-Folgen: Zusatzkosten größte Sorge, Lieferkette und Belegschaft kaum
Mit Blick auf die Folgen eines Cyberangriffs, gilt die in deutschen Chefetagen meistgenannte Sorge den dadurch entstehenden Kosten – etwa durch eine notwendige Wiederherstellung

des Geschäftsbetriebs. Die möglichen Unterbrechungen der kaufmännischen Abläufe stehen am zweithäufigsten im Fokus.

Ein Interessanter Aspekt hierbei: Probleme im Rahmen der Lieferketten vermuten insgesamt noch weniger Befragte (23 Prozent) als einen möglichen Imageverlust (28 Prozent). Allein im verarbeitenden Gewerbe, und das ist keine große Überraschung, gehen immerhin insgesamt knapp 37 Prozent der Befragten davon aus, dass die Lieferketten möglicherweise betroffen sein könnten.

Dem Verlust von Kunden oder Beschäftigten als Folge von Cyberattacken messen die Führenden hingegen kaum bis keine Bedeutung bei: Mit Kundenverlusten rechnen 19,4 Prozent und noch weniger (1,5 Prozent) befürchten, Mitarbeitende zu verlieren.

Auch Zahlungsunfähigkeit (9,5 Prozent) und Bußgelder wegen Datenschutzverletzungen (5,5 Prozent) werden kaum als Risiken gesehen, lediglich in der Schweiz regt sich hier etwas mehr Sorge: hier erwarten knapp 22 Prozent eine Zahlungsunfähigkeit sowie 11,8 Prozent Bußgeldzahlungen als mögliche Folgen von Cyberattacken.

Chester Wisniewski: International (leider) ein ähnliches Bild
„Die Ergebnisse in der DACH-Region sind zwar enttäuschend, entsprechen aber dem, was wir in Nordamerika, ASEAN und anderen Regionen beobachten“, kommentiert Chester Wisniewski, Principal Research Scientist bei Sophos die Ergebnisse der Studie. „Leider wird die Sicherheit, wenn sie als Bestandteil der IT verwaltet wird, in der Regel auf den Status einer Aufgabe zurückgestuft, anstatt eine Priorität zu sein. Die Rolle des Sicherheitsteams besteht darin, Risiken zu identifizieren und dem Vorstand dabei zu helfen, diese Risiken nach Prioritäten zu ordnen, wohingegen die IT-Abteilung die Aufgabe hat, die erforderlichen Änderungen zu implementieren, je nachdem, wie diese Risiken angegangen werden sollen.“

Auch, was die Bedeutung der IT-Sicherheit vor dem Hintergrund der weltpolitischen Lage angeht, scheint weltweit einhellige Gelassenheit zu sorgen. Wisniewski: „Der Krieg in der Ukraine hat die Einstellungen nicht wirklich verändert, abgesehen von den kritischen US-Infrastrukturen. Die US-amerikanische CISA-Agentur hat ihre Bemühungen zur Verbesserung des Sicherheitsbewusstseins und in einigen Fällen der Meldepflichten für Anbieter kritischer Infrastrukturen verstärkt, aber außerhalb der USA oder in anderen Unternehmen des privaten Sektors sind keine großen Bedenken oder Maßnahmen zu erkennen.“

Über die Umfrage:
Ipsos hat im Auftrag von Sophos 201 C-Level-Managerinnen und -Manager aus Handel, Dienstleitung und verarbeitendem Gewerbe in Deutschland sowie jeweils 50 in Österreich und der Schweiz zum Thema IT-Sicherheit in ihren Unternehmen befragt.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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