Weltweite Ransomware-Studie von Sophos: Wer zahlt, zahlt drauf

- *Lösegeld-Zahlungen nach Ransomware-Attacken ziehen fast das Doppelte an Kosten für die Wiederbeschaffung verschlüsselter Daten nach sich*
- *Deutsche Unternehmen im europäischen Vergleich am zweitstärksten von Ransomware betroffen*
- *E-Mails hierzulande Einfallstor Nummer Eins*

Wiesbaden, 12. Mai 2020 – Sophos hat heute die Ergebnisse seiner globalen Studie „The State of Ransomware 2020" bekannt gegeben. Die Studie zeigt unter anderem, dass die Zahlung von Lösegeldern für die Wiederherstellung von Daten, die während eines Ransomware-Angriffs verschlüsselt wurden, nicht die einfachste und günstigste Lösung ist. Tatsächlich verdoppeln sich die Gesamtkosten der Wiederherstellung nahezu, wenn Organisationen ein Lösegeld zahlen. Für die Umfrage wurden 5.000 IT-Entscheidungsträger aus Organisationen in 26 Ländern auf sechs Kontinenten befragt, darunter Europa, Amerika, Asien-Pazifik und Zentralasien, der Nahe Osten und Afrika.

Mehr als die Hälfte (51 Prozent) der Organisationen haben in den vergangenen 12 Monaten einen Lösegeldangriff erlebt. Bei fast drei Vierteln (73 Prozent) der Angriffe, bei denen es gelang, in eine Organisation einzudringen, wurden Daten verschlüsselt. Die durchschnittlichen Kosten für die Bewältigung der Auswirkungen eines solchen Angriffs ohne die Zahlung von Lösegeld betrugen mehr als 730.000 Dollar, Geschäftsausfallzeiten, verlorene Aufträge, Betriebskosten etc. eingerechnet. Wurde das Lösegeld gezahlt, stiegen die Durchschnittskosten mit 1,4 Millionen Dollar sogar fast auf das Doppelte.

Indische Unternehmen zahlen am häufigsten, italienische am seltensten
Mehr als ein Viertel (27 Prozent) der von Lösegelderpressung betroffenen Organisationen gaben zu, das erpresste Geld gezahlt zu haben. Hier zeigte sich, dass besonders indische Unternehmen (zu 66 Prozent) bereit waren, für die Herstellung der Daten zu bezahlen, gefolgt von schwedischen (50 Prozent), belgischen (32 Prozent) und japanischen (31 Prozent). Am wenigsten geneigt, den Forderungen der Kriminellen nachzukommen, waren Unternehmen aus Spanien (4 Prozent) und Italien (5 Prozent). Auch die deutschen Unternehmen zählten mit nur 12 Prozent Lösegeld-Bereitschaft zu den Zahlungsunwilligen.

"Organisationen können dem Druck erliegen, ein Lösegeld zu zahlen, um schädliche Ausfälle zu vermeiden. Auf den ersten Blick erscheint dies auch als ein wirksames Mittel zur Wiederherstellung der von den Angreifern verschlüsselten Daten. Doch die Realität sieht anders aus," sagt Chester Wisniewski, Principal Research Scientist bei Sophos.

Backup statt Bitcoins – Lösegeldzahlungen nicht das wirksamste Mittel
Die Ergebnisse der Studie zeigen, dass die Zahlung des Lösegelds die Wiederherstellungslast in Bezug auf Zeit und Kosten kaum beeinflusst. „Dies könnte daran liegen, dass es unwahrscheinlich ist, die Daten mit nur einem einzigen Entschlüsselungsschlüssel wiederherzustellen. Häufig teilen sich die Angreifer mehrere Schlüssel und deren Verwendung für die Daten-Rekonstruktion kann eine komplexe und zeitaufwändige Angelegenheit sein", so Wisniewski weiter. Zudem zeigte sich im Rahmen der Studie, dass mehr als die Hälfte (56 Prozent) der befragten IT-Manager auch ohne Lösegeldzahlung in der Lage waren, ihre Daten aus Backups wiederherzustellen. In einer sehr kleinen Minderheit der Fälle (1 Prozent) führte die Zahlung des Lösegeldes nicht zur Wiederherstellung der Daten.

Bei Organisationen des öffentlichen Sektors stieg diese Zahl auf 5 Prozent. Tatsächlich gelang es 13 Prozent der befragten Organisationen des öffentlichen Sektors nie, ihre verschlüsselten Daten wiederherzustellen, verglichen mit 6 Prozent insgesamt. Entgegen der landläufigen Meinung war der öffentliche Sektor dabei am wenigsten von Lösegeldforderungen aus Ransomware-Attacken betroffen, da nur 45 Prozent der in dieser Kategorie befragten Organisationen angaben, einem Angriff ausgesetzt gewesen zu sein. Auf globaler Ebene waren Medien-, Freizeit- und Unterhaltungsunternehmen im privaten Sektor am stärksten betroffen, hier berichteten 60 Prozent der Befragten von Angriffen.

Deutschland im europäischen Vergleich am zweitstärksten betroffen

Am stärksten von Ransomware-Angriffen betroffen war Indien, wo 82 Prozent der befragten Unternehmen eine Attacke bestätigten. Am wenigsten ausgesetzt zeigten sich Unternehmen in Südafrika mit nur 24 Prozent. Die USA waren mit 59 Prozent weltweit am sechst häufigsten betroffen. Im europäischen Vergleich lagen nur Belgien und Schweden (beide 60 Prozent) vor Deutschland, wo 57 Prozent der befragten Unternehmen einen Angriff bestätigten. Weltweit bedeutet dieser Wert Position acht. Andere europäische Nachbarn wie die Niederlande, Spanien oder Frankreich liegen bei Werten von rund 55 bis 53 Prozent, Unternehmen des Vereinigten Königreichs bestätigten zu 48 Prozent angegriffen worden zu sein. Polen hatte laut der Studie mit 28 Prozent europaweit die wenigsten Erpressungs-Attacken zu verzeichnen.

E-Mails in deutschen Firmen erfolgreichste Schleuse für Ransomware

Die Schadware ist auf unterschiedlichen Wegen in die Unternehmen gelangt. Haupteinfallstor waren dabei bösartige Links und File-Downloads, über die die Erpressungssoftware heruntergeladen wurde. Weltweit lag dieser Wert bei 29 Prozent, in Deutschland sogar bei 41 Prozent. Per E-Mail wurde die Ransomware in Deutschland zu 22 Prozent durch schadhafte Anhänge (ein Spitzenwert im internationalen Vergleich) in die Firmen geschleust. Für Unternehmen hierzulande erweisen sich also E-Mails als das Haupteinfallstor für diese Schadware. Gut steht Deutschland bei einem anderen Vergleich da: Remote-Attacken auf Server fielen hier nur 13 Prozent der Unternehmen zum Opfer, international lag dieser Wert bei 21 Prozent.

Über die Studie

Die Umfrage „State of Ransomware 2020“ wurde von Vanson Bourne, einem unabhängigen Spezialisten für Marktforschung, im Januar und Februar 2020 durchgeführt. Im Rahmen der Umfrage wurden 5.000 IT-Entscheidungsträger in 26 Ländern befragt, und zwar in den USA, Kanada, Brasilien, Kolumbien, Mexiko, Frankreich, Deutschland, Großbritannien, Italien, den Niederlanden, Belgien, Spanien, Schweden, Polen, der Tschechischen Republik, der Türkei, Indien, Nigeria, Südafrika, Australien, China, Japan, Singapur, Malaysia, den Philippinen und den Vereinigten Arabischen Emiraten. Alle Befragten stammten aus Organisationen mit 100 bis 5.000 Mitarbeitern.

Über Sophos

Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. 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