Cyberversicherung ist nicht nur eine Frage der Unternehmensstrategie, sondern auch, ob man eine bekommt

Sophos hat einen neuen Leitfaden zu Cyberversicherungen veröffentlicht, der dem Management und IT-Verantwortlichen in Unternehmen hilft, den Markt der Cyberversicherungen besser zu verstehen und die Voraussetzungen für eine möglichst wirtschaftliche Versicherung zu erfüllen.

Unternehmen sichern sich häufig zusätzlichen zur technischen Security durch eine Cyberversicherung ab. Hinter dieser Strategie steckt einerseits das Wissen um die Gefahr mit einer eventuell rückständigen Inhouse-Security und andererseits ein betriebswirtschaftliches Kalkül der Führungsetage. Klar ist, dass im letzten Sophos State of Ransomware Reports 49 Prozent der in Deutschland (70 Prozent in Österreich und 60 Prozent in der Schweiz) Befragten bestätigen, dass es eine Datenverschlüsselung im Unternehmen durch Ransomware gab. Das Risiko ist existent. Und klar ist auch, dass eine Cyberversicherung die Gesamtkosten eines solchen Vorfalls, die ein Vielfaches der Erpressungssumme betragen, erträglicher machen kann. Immerhin belaufen sich die weltweit durchschnittlichen Gesamtkosten zur Wiederherstellung exklusive der Lösegeldzahlung nach einer Attacke auf 1,82 Millionen US-Dollar. 1,54 Millionen US-Dollar betrug die durchschnittliche Lösegeldsumme, fast doppelt so viel wie im Vorjahr mit 812,380 Millionen US-Dollar.

Allerdings sind die Kosten einer Cyberversicherung aufgrund der vielen Schadensfälle in den letzten Jahren stark gestiegen und die Kriterien, um einen Versicherungsschutz überhaupt zu bekommen, stellen für Unternehmen mittlerweile große Hürden dar. Der neue Leitfaden für Cyberversicherungen von Sophos gibt Hilfestellung und klärt auf, wie Unternehmen mit moderner Cybersecurity einen besseren Versicherungsstatus zu günstigeren Prämien oder überhaupt eine Police bekommen. Neben aktuellen Vergleichen, ob der Versicherungsschutz in unterschiedlichen Branchen innerhalb der Unternehmensversicherung oder als gesonderte Versicherung abgedeckt ist, den Kosten für die Versicherungsleistungen sowie dem Markt für Cyberversicherungen, gibt Sophos praktische Tipps, um den Schutz zu guten Konditionen zu erreichen. Dazu gehören vier entscheidende Aspekte:

Mehrstufige Authentifizierung (MFA)
Eine grundlegende Anforderung ist das Etablieren einer mehrstufigen Authentifizierung (MFA) im gesamten Unternehmen und für alle Anwendungen. Damit möchten Versicherer sichergehen, dass gängige Sicherheitslücken geschlossen werden, bevor sie Risiken übernehmen.

Endpoint Detection and Response (EDR) oder Extended Detection and Response (XDR)
Fortschrittlicher Endpoint-Schutz ist die wesentliche Grundlage für eine starke Cyberabwehr. Um modernste Ransomware und Sicherheitsverletzungen (und damit auch Schadensfälle) abzuwehren, ist es zusätzlich wichtig, proaktiv nach verdächtigen Aktivitäten zu suchen, diese zu analysieren und darauf zu reagieren, bevor Cyberkriminelle ihren Angriff ausführen können. Mit EDR- und XDR-Programmen können Sicherheitsspezialisten potenzielle Kompromittierungen erkennen und analysieren und komplexe Cyberangriffe so bereits beseitigen, bevor Schaden entsteht. Die meisten Cyberversicherer setzen EDR für eine Versicherungsleistung voraus.

Managed Detection and Response (MDR)
MDR ist ein 24/7 Fully-Managed Service, der durch ein Team von Sicherheitsexperten bereitgestellt wird. Diese sind auf das Erkennen und Bekämpfen von Cyberangriffen spezialisiert, gegen die reine Technologie-Lösungen machtlos sind. Der Service minimiert das Risiko und die Wahrscheinlichkeit, die Versicherung in Anspruch nehmen zu müssen. Zwar wird Managed Detection and Response (MDR) von Versicherern nicht zwingend vorausgesetzt, allerdings gelten Unternehmen, die MDR-Services nutzen, häufig als Premium-Kunden, da sie das geringste Risiko darstellen.

Incident-Response-Plan
Vorbereitung ist die beste Strategie, um zu verhindern, dass sich ein Cyberangriff zu einem weitreichenden Sicherheitsvorfall entwickelt. Nach einer Sicherheitsverletzung stellen Unternehmen oft fest, dass ein Incident-Response-Plan viele Kosten, Probleme und Betriebsunterbrechungen erspart hätte. Ein detaillierter Plan, mit dem die Folgen eines Vorfalls abmildert werden, reduziert das Cyberrisiko und macht das Unternehmen für Versicherungsanbieter attraktiver.

Der neue Sophos Guide zu Cyberversicherungen steht im Sophos Partnerportal zum Download bereit.

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/
X/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
Ariane Wendt +49-172-4536839
sophos@tc-communications.de