Unternehmensmeldung

HDI Versicherung AG

Hannover, 12.04.2022

Cyberangriffe und Schäden bei KMU - Ergebnisse der HDI Cyber-Studie

- **Angriffe in erster Linie über die Schwachstelle „Mensch“**
- **Durchschnittliche Schadenhöhe: 95.000 EUR**
- **Entdeckung der Attacken oft nur durch Zufall oder Schaden**
- **Viele wechseln nach Cyberangriff den IT-Dienstleister**

Die Anzahl von Cyberattacken gegen Unternehmen ist in den vergangenen Jahren immer weiter gestiegen. Mehr als eine Million der rund 3,5 Millionen kleinen und mittelständischen Unternehmen (KMU) in Deutschland hat in den letzten Jahren bereits Cyberangriffe gegen das eigene Unternehmen erfahren müssen. Vor allem unter den Mittelständlern mit 50 bis 250 Mitarbeitern berichtet mehr als jedes zweite Unternehmen (57%), schon mindestens einmal von einer Cyber-Attacke betroffen gewesen zu sein. Das sind Ergebnisse der aktuellen HDI Cyber-Studie, zu der Versicherungs- und IT-Entscheider von mehr als 500 KMU in Deutschland durch das Forschungs- und Beratungsinstitut Sirius Campus repräsentativ befragt wurden.

Fast drei Viertel der erfolgreichen Angriffe (72%) verursachen dabei erhebliche Schäden und kosten KMU im Schnitt 95.000 EUR. Bei Freiberuflern liegt der Schadendurchschnitt laut Studie sogar bei 120.000 EUR und größere Mittelständler berichten von Schäden von bis zu 500.000 Euro. Dass laut Untersuchung Mittelständler überdurchschnittlich betroffen waren, heißt jedoch nicht, dass kleinere und Kleinstunternehmen für die Angreifer nicht interessant sind. Auch rund ein Drittel (31%) der Kleinstunternehmen mit bis zu 9 Mitarbeitern und 37 Prozent der Kleinunternehmen mit

10 bis 49 Mitarbeitern sind in den letzten Jahren bereits Opfer von Cyber-Attacken geworden.

„Die häufig geäußerte Ansicht, dass kleinere Unternehmen für Cyber-Angriffe nicht interessant seien, ist durch die Praxis klar widerlegt", sagt dazu Christian Kussmann, Bereichsvorstand Firmen und Freie Berufe der HDI Versicherung AG. Zudem zeige sich ein genereller Trend: Kleinere Unternehmen gerieten verstärkt in den Fokus seitdem sich größere Unternehmen besser gegen solche Angriffe schützten. KMU haben dagegen häufig nicht so hohe Sicherheitshürden wie große Unternehmen. Außerdem nutzen Angreifer die KMU auch als „Point of Entry" für weitere Angriffe. Denn als Dienstleister unterhalten sie häufig auch IT-Schnittstellen zu Großunternehmen.

Angriffe hauptsächlich über Schwachstelle „Mensch"

Angriffe über erweiterte Computer- oder IoT-Netzwerke oder über Wartungsschnittstellen von Druckern oder Kopierern – Angriffsmethoden werden immer ausgefeilter und technisch anspruchsvoller. Allerdings sind es bislang relativ wenige Unternehmen, die in der Praxis bereits auf diese Weise attackiert wurden. Im Schwerpunkt zielen die Angriffsmethoden weiterhin klar auf die Schwachstelle Mensch. So geben 20 Prozent der Unternehmen an, dass sie bereits durch Vortäuschen falscher Identitäten, Spam- oder Phishing-Mails attackiert wurden. Fast genauso viele wurden über verseuchte Anhänge in E-Mails an Mitarbeiter und Schadsoftware angegriffen. „Die Untersuchungsergebnisse zeigen klar: Angreifer wählen den Weg des geringsten Widerstands. Beim allergrößten Teil der Angriffe nutzen Angreifer Unaufmerksamkeit, Neugier oder Arglosigkeit bei Mitarbeitern, um in die IT-Netzwerke der Firmen einzudringen," ergänzt HDI Vorstand Kussmann. Technisch anspruchsvollere Angriffsmethoden gälte es trotzdem weiter im Fokus zu behalten und technische sowie organisatorische Gegenmaßnahmen zu ergreifen.

Betriebsunterbrechungen und Diebstahl von Kundendaten

Rund ein Viertel der betroffenen Unternehmen (24%) musste laut Untersuchung mit Betriebsunterbrechungen in Folge der Attacken

klarkommen, so die Studien-Ergebnisse. Zum Beispiel konnte ein Unternehmen aufgrund der kompromittierten Systeme seine Kunden vorübergehend nicht beliefern. Ein anderes konnte nicht mehr auf E-Mails und Firmennetzwerk zugreifen. Buchführung und Kundenservice waren lahmgelegt. Nicht umsonst werden Betriebsunterbrechungen deshalb von 43 Prozent der Unternehmen als besonders relevant eingestuft.

Als noch relevanter bewerten die befragten Unternehmen nur den Diebstahl von Kundendaten: 45 Prozent der Befragten sahen hier eine große Relevanz und fast jedes vierte der angegriffenen Unternehmen (22%) war bereits betroffen. Genauso häufig sind Auswirkungen auf den Ruf des Unternehmens: 22 Prozent der attackierten Unternehmen beklagen Image- und Reputationsschäden infolge der Cyberangriffe. Zudem sahen sich 15 Prozent mit Schadenersatzforderungen von Kunden konfrontiert und 16 Prozent mit Industriespionage und dem Verlust geheimer Unterlagen.

Betriebsunterbrechungen treiben die Schadenkosten in die Höhe

Betriebsunterbrechungen erweisen sich auch als wichtiger Treiber der Schadenhöhe. Bei mehr als der Hälfte der betroffenen Unternehmen war der Betrieb laut Studie für mindestens zwei Tage eingeschränkt. Rund 15 Prozent mussten sogar mit 4 bis 7 Tagen Betriebsstörungen klarkommen. Besonders hart getroffen wurden dabei Kleinstunternehmen. Denn allein das Entfernen von Schadsoftware und das Einspielen von Updates ist in komplexen IT-Systemen von heute nicht in ein paar Stunden erledigt, auch nicht in kleineren Unternehmen. Ein Studienteilnehmer beschreibt die Situation so: "Eine als legal propagierte Software stellte sich als Schadsoftware heraus und war extrem schwierig zu entfernen. Sämtliche Softwaretools zur Behebung waren unwirksam. Die Beseitigung war nur möglich im abgesicherten Modus des Betriebssystems und durch manuelles Entfernen jeder einzelnen Datei."

Angriffe häufig nur zufällig entdeckt

Häufig werden Cyberangriffe bei kleinen und mittelständischen Unternehmen nur zufällig entdeckt. Auch das ist ein Ergebnis aus der Cyberstudie. HDI Vorstand Kussmann warnt: „Wenn eine

Schadsoftware lange unerkannt im System bleibt, besteht häufig die Gefahr, dass die besonders schwerwiegende Schäden anrichtet." Das Ziel müsse daher sein, Angriffe frühzeitig zu erkennen und Schadsoftware unschädlich zu machen. Insgesamt gaben jedoch 28 Prozent der betroffenen KMU an, dass Cyberattacken nur durch Zufall entdeckt wurden. Bei Kleinst- und Kleinunternehmen war dies sogar bei jeweils rund einem Drittel der Firmen der Fall.

Mittelständische Unternehmen entdeckten Cyber-Angriffe dagegen zum großen Teil durch systematisches Screening. Neben der Überprüfung veröffentlichter Schwachstellen gehört das Screening zu den erfolgversprechendsten Methoden, Cyberattacken möglichst frühzeitig zu bemerken und Gegenmaßnahmen einleiten zu können. Kleinere Unternehmen haben hier oft erheblichen Nachholbedarf. Besonders schlecht für Unternehmen ist dagegen, wenn Cyberangriffe erst durch die Schäden, die sie anrichten, bemerkt werden. Etwa ein Fünftel der von Cyberattacken betroffenen Unternehmen musste bereits derartige Erfahrungen machen. Mit 17 Prozent etwas weniger bei den Mittelständlern, bei kleineren Unternehmen mehr.

Einsatz von Spezialisten und Austausch des IT-Dienstleisters

Bei der Schadenbeseitigung kam meistens ein unternehmenseigenes Team oder der interne Verantwortliche für Informationssicherheit der Unternehmen zum Einsatz. Rund die Hälfte der attackierten Unternehmen setzen bei der Schadenbeseitigung auf interne Kräfte. Zum Beispiel trennt in einem solchen Fall ein speziell geschultes Team das kompromittierte System vom Netzwerk und setzt das System neu auf, spielt ein Backup ein oder entfernt die Schadsoftware. Anschließend werden ein FullScan der Systeme und weitere forensische Untersuchungen durchgeführt. 38 Prozent überließen die Aufgabe ihrem IT-Dienstleister. Außerdem gaben 30 Prozent der Betroffenen an, IT-Spezialisten der Cyberversicherung zu Rate gezogen zu haben.

Die Härtung der eigenen Systeme mit neuer Soft- und Hardware sowie zusätzlichen Präventionsmaßnahmen standen nach einer Cyber-Attacke bei vielen im Fokus: jeweils über ein Drittel Unternehmen entschieden sich für mindestens einen dieser Schritte.

Dass Cyberangriffe zu Schäden führten, hatte häufig auch Auswirkungen auf die Zusammenarbeit mit IT-Dienstleistern: Für rund ein Fünftel der bisherigen IT-Dienstleister bedeutete es das Aus beim attackierten Unternehmen: 21 Prozent der Unternehmen wechselten in der Folge den IT-Dienstleister.

Als Konsequenz der erlittenen Cyber-Attacke entschieden sich außerdem über ein Viertel der betroffenen Unternehmen für den Abschluss einer Cyber-Versicherung. Denn gerade nach größeren Schäden tritt die Frage nach einem möglichen Versicherungsschutz in den Fokus. Nur bei einem Viertel der Schadenfälle war der Schaden umfassend durch eine Cyber-Versicherung abgesichert. 30 Prozent der Befragten verfügten dagegen über keinerlei Versicherungsschutz für den erlittenen Schaden. HDI Vorstand Kussmann erläutert: „Integrierte Präventions- und Versicherungsangebote für den Schutz gegen Cyber-Attacken bieten gerade für KMU einen komfortablen Rundum-Service. Denn neben dem finanziellen Ausgleich von Schäden stehen dabei auch wirksame Präventionsmaßnahmen und Mitarbeiterschulungen im Fokus, die Schadenwahrscheinlichkeit und Schadenhöhe erheblich senken können."

Für weitere Presseinformationen:
Talanx Group Communications
HDI Versicherungen
Andreas Ahrenbeck
Telefon: +49 511 645-4746
presse@hdi.de

Die HDI Versicherung AG bietet Sachversicherungslösungen für Privat- und Firmenkunden. Dabei reicht die Angebotspalette von Kfz-Versicherungen über private Haftpflicht- und Hausratversicherungen bis hin zu Komplettlösungen für kleine und mittlere Unternehmen sowie speziellen, berufsbezogenen Lösungen für Freie Berufe. Die HDI Versicherung AG gehört zur Talanx-Gruppe.

Die Talanx ist mit Prämieneinnahmen in Höhe von 45,5 Mrd. EUR (2021) und rund 24.000 Mitarbeiterinnen und Mitarbeitern eine der großen europäischen Versicherungsgruppen. Die Talanx AG ist an der Frankfurter Börse im MDAX sowie an der Börse in Hannover (ISIN: DE000TLX105, WKN: TLX100) gelistet.