KRIMINOLOGISCHES FORSCHUNGSINSTITUT NIEDERSACHSEN E.V.

Leibniz Universität Hannover

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Pressemitteilung

Hannover, 13.09.2021

Risiko von Cyberangriffen steigt

Das Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) veröffentlicht Ergebnisse einer Folgebefragung von Unternehmen zum Thema Cyberkriminalität. Insbesondere Angriffe mit Schadsoftware und Phishing nahmen im letzten Jahr sehr deutlich zu, während die IT-Sicherheit von Unternehmen durch die Corona-Krise beeinträchtigt wurde.

Drei Fünftel (60 %) der 635 im Jahr 2020 erneut befragten Unternehmen musste innerhalb eines Jahres auf mindestens einen Cyberangriff reagieren. Damit stieg die Betroffenheit innerhalb eines Jahres im Vergleich zur ersten Befragung (2018/19) bei den teilnehmenden Unternehmen um 10 Prozentpunkte. *„Neben dem Anteil der Betroffenheit nahm auch die durchschnittliche Anzahl der erlebten Angriffe innerhalb von zwölf Monaten insbesondere bei Phishing-Angriffen sehr deutlich zu“*, sagt der Soziologe Arne Dreißigacker (Projektleiter). Zudem wirkte sich vor allem bei Unternehmen mit angespannter wirtschaftlicher Situation die Corona-Krise nach Einschätzung der befragten Unternehmensvertreter*innen häufig negativ auf die IT-Sicherheit aus. Homeoffice und die Nutzung privater Hard- und Software erhöhen das Risiko von Phishing und Angriffen mit Schadsoftware. Die Anzeigequote bleibt weiterhin sehr gering. Nur jedes zwölfte betroffene Unternehmen (8,5 %) zeigte den berichteten schwerwiegendsten Cyberangriff der letzten zwölf Monate an. Die Fallzahlen der Polizeilichen Kriminalstatistik (PKS) bilden also nur einen Bruchteil des tatsächlichen Ausmaßes ab. Dies gehört zu den zentralen Befunden der zweiten Unternehmensbefragung innerhalb des Forschungsprojektes „Cyberangriffe gegen Unternehmen“, welche das Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) am 13.09.2021 vorlegt.

Auch wenn grundlegende technische IT-Sicherheitsmaßnahmen, wie Firewall, regelmäßige Backups, aktuelle Antivirensoftware und regelmäßige Sicherheitsupdates und Patches mittlerweile in fast allen Unternehmen zum Einsatz kommen, ließen sich große Unterschiede hinsichtlich des Reifegrades solcher Maßnahmen feststellen. Zwar setzen z.B. 98 % der Unternehmen aktuelle Antivirensoftware ein, allerdings nutzt jedes achte Unternehmen (12 %) lediglich die Grundfunktionalität/ den Grundumfang der verwendeten Software, ohne diese/n in Hinblick auf die eigenen Anforderungen regelmäßig zu überprüfen bzw. zu optimieren. Das mit den Befragungsdaten entwickelte Tool CARE (https://www.cybercrime-forschung.de/care) bietet insbesondere kleinen und mittleren Unternehmen eine individuelle Risikoeinschätzung und gibt Handlungsempfehlungen zur Verbesserung der IT-Sicherheit.

Das Projekt „Cyberangriffe gegen Unternehmen“ wurde zusammen mit dem Forschungszentrum L3S der Leibniz-Universität Hannover durchgeführt und im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (BMWi) gefördert. Eine Zusatzförderung erfolgte von der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC) sowie der VHV Stiftung. Die detaillierten Ergebnisse, weitere Informationen zum Projekt oder zum methodischen Vorgehen der Befragung finden sich im KFN-Forschungsbericht Nr. 162, der auf der Webseite des KFN zur Verfügung steht:

https://kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf

Ansprechpartner:

Arne Dreißigacker, Soziologe, KFN e.V.
E-Mail: arne.dreissigacker@kfn.de;
Tel.: +49 (511) 34836-28

Zusatzförderung durch: pwc VHV STIFTUNG

Das Forschungsprojekt „Cyberangriffe gegen Unternehmen“

Das KFN führte zusammen mit dem Forschungszentrum L3S der Universität Hannover von Dezember 2017 bis März 2021 ein umfangreiches Forschungsprojekt zum Thema „Cyberangriffe gegen Unternehmen“ durch. Das Projekt wurde finanziert durch die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (www.it-sicherheit-in-der-wirtschaft.de) sowie durch eine Zusatzförderung von der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers und der VHV-Stiftung. Neben einer großangelegten repräsentativen Befragung von 5.000 Unternehmen ab 10 Beschäftigten im Jahr 2018/19 und einer webbasierten Folgebefragung im Jahr 2020 wurde durch Feldstudien analysiert, wie gut bestehende Handlungsleitlinien von den jeweiligen IT-Beauftragten in Unternehmen umgesetzt werden können und wie diese bei Vorfällen vorgehen, um Angriffe richtig zu erkennen und entsprechend zu reagieren.

Methode und Stichprobe der Unternehmensbefragungen

Die erste Befragung von 5.000 Unternehmen wurde per computergestützten Telefoninterviews (CATI) zwischen August 2018 und Januar 2019 durchgeführt. Die Folgebefragung, an der insgesamt 687 Unternehmen erneut teilnahmen, erfolgte zwischen Juli und September 2020 als Web Survey.

Der eingesetzte standardisierte Fragebogen enthielt 57 Fragen zur Risikoeinschätzung, zu erlebten Cyberangriffen, zu IT-Sicherheitsmaßnahmen, zu Unternehmensmerkmalen, zum Anzeigeverhalten und zur veränderten Situation in der Corona-Krise.

Die Befragung basiert auf einer geschichteten Zufallsstichprobe aus zwei Unternehmensdatenbanken und umfasst Unternehmen ab zehn Beschäftigten nahezu aller Branchen der offiziellen Klassifikation der Wirtschaftszweige (WZ08-A bis S). Interviewpartner*innen waren vor allem IT-Verantwortliche und Mitglieder der Geschäftsführung. Durch eine nachträgliche Gewichtung der geschichteten Zufallsstichprobe nach Beschäftigtengrößenklasse und Wirtschaftszweig entspricht die Verteilung der Zusammensetzung aller Unternehmen ab zehn Beschäftigten in Deutschland, womit verallgemeinerbare Aussagen für diese Gruppe möglich sind. Bei der Interpretation der zentralen Ergebnisse, die sich im Folgenden auf alle Unternehmen der Stichprobe beziehen, ist demzufolge zu berücksichtigen, dass kleine Unternehmen mit 10-49 Beschäftigten den größten Anteil (79 %) bilden, wohingegen große Unternehmen mit mehr als 500 Beschäftigen lediglich 2 % in der gewichteten Stichprobe ausmachen.

Zentrale Ergebnisse der Folgebefragung

Einschätzung des Unternehmensrisikos von Cyberangriffen fällt pessimistischer aus

Die Hälfte der Unternehmen schätzt das Risiko eines schädigenden ungezielten Cyberangriffs in den nächsten zwölf Monaten für sehr/eher hoch ein. Im Vergleich zur ersten Befragung (2018/19) nahm dieser Anteil um 14 Prozentpunkte zu. Demgegenüber nahm die Gruppe der Unternehmen, die dieses Risiko für sehr gering halten, anteilig von 14 % auf 5 % ab.

Betroffenheit von Cyberangriffen steigt

Über alle Angriffsarten hinweg waren etwa drei Fünftel der Unternehmen ab 10 Beschäftigten (60 %) in den letzten zwölf Monaten (immer bezogen auf die Zeit vor der Befragung) von mindestens einem Cyberangriff betroffen, auf den in irgendeiner Weise aktiv reagiert werden musste. Automatisiert abgewehrte Angriffe, z.B. Spam-E-Mails durch eine Firewall, sind hier nicht enthalten. Unterschieden nach Angriffsarten zeigt sich, dass vergleichsweise viele Unternehmen in den letzten zwölf Monaten von Phishing (42 %) und Schadsoftwareangriffen (Ransomware: 14 %, Spyware: 16 % und sonstige Schadsoftware: 36 %) betroffen waren, gefolgt von CEO-Fraud (11 %), (D)DoS (8 %), Defacing und manuellem Hacking (1 % bzw. 0,4 %). Im Vergleich mit den Ergebnissen der ersten Befragung hat vor allem die Betroffenheit von Angriffe mit sonstiger Schadsoftware (+ 10 Prozentpunkte) und Phishing (+ 17 Prozentpunkte) deutlich zugenommen. Dies ist tendenziell in allen Beschäftigtengrößenklassen zu erkennen.

Spannbreite der Kosten durch Cyberangriffe bleibt groß

Für die Beantwortung weiterer Detailfragen sollten die befragten Unternehmen den schwerwiegendsten Angriff der letzten zwölf Monate auswählen.

In der überwiegenden Mehrzahl blieben die berichteten schwerwiegendsten Cyberangriffe anscheinend in einem frühen Versuchsstadium stecken (85 %). Lediglich ein Anteil von 7 % berichtete von einem aus Sicht der Täter*innen erfolgreichen und weitere 8 % von einem teilweise erfolgreichen Angriff. Dennoch sind bei der Hälfte der betroffenen Unternehmen direkte Kosten im Zusammenhang mit dem schwerwiegendsten Cyberangriff entstanden. Am häufigsten wurden Personalkosten für die Behebung des Problems (40 %), Kosten durch externe Beratung (22 %) und Kosten zur Wiederbeschaffung bzw. Wiederherstellung von Soft- und Hardware (17 %) genannt.

Erneut zeigte sich, dass die Spannbreite der direkten Kosten, die durch die berichteten schwerwiegendsten Cyberangriffe der vergangenen zwölf Monate verursacht wurden, sehr groß ist (20 EUR bis 3,8 Mio. EUR), die Kosten mehrheitlich aber relativ gering ausfielen (Durchschnitt: 7.890 EUR, Median: 500 EUR). Dies wird durch die Einschätzung der befragten Unternehmen zu den entstandenen materiellen und nicht-materiellen Schäden gestützt. Insgesamt betrachtet gaben 47 % an, dass kein Schaden entstanden ist, 51 % schätzten diese als kurzfristig/gering ein und lediglich 2 % als mittelfristig/deutlich spürbar. Vorfälle mit schwerwiegenden kostenintensiven Folgen bzw. langfristigen/bestandsgefährdenden Schäden scheinen demnach selten zu sein.

Anzeigebereitschaft nach wie vor gering

Bezogen auf den schwerwiegendsten Cyberangriff der letzten zwölf Monate gaben nur 9 % der Unternehmen an, diesen polizeilich angezeigt zu haben. Damit bleibt die Anzeigequote auch in der Folgebefragung auf einem sehr niedrigen Niveau (in der ersten Befragung lag sie bei 12 %).

Die Anzeige von Cyberangriffen steht im Zusammenhang mit der Frage, ob der Angriff aus Sicht der Täter*innen zumindest teilweise erfolgreich war. So zeigten immerhin ein Viertel der Unternehmen (26 %) den schwerwiegendsten Angriff an, die diese Frage bejahten, wohingegen nur 6 % Anzeige erstatteten, bei denen die Täter*innen keinen Erfolg hatten.

Die am häufigsten genannten Nichtanzeigegründe sind die geringe Schadenshöhe (82 %), die fehlende Aussicht auf einen Ermittlungserfolg (53 %) und die Unsicherheit, an wen man sich dafür wenden muss (17 %). Befürchtungen von Imageschäden (0,3 %), Arbeitsbehinderungen (2 %) oder von behördlicher Einsicht in vertrauliche Daten (1 %) spielen demgegenüber nur eine untergeordnete Rolle.

Corona-Krise beeinträchtigt IT-Sicherheit

Vor der Corona-Krise gab es in knapp der Hälfte der Unternehmen (47 %) die Möglichkeit zu Homeoffice und in etwa jedem fünften Unternehmen (22 %; N=533) konnte private Soft-/Hardware zu dienstlichen Zwecken genutzt werden. Diese Anteile nahmen mit der Corona-Krise signifikant auf 68 % bzw. 31 % zu. Gleichzeitig verschlechterte sich in vielen Unternehmen die wirtschaftliche Situation: Während nur 16 % der Unternehmen die wirtschaftliche Situation des Unternehmens für die Zeit vor der Corona-Krise als (eher) angespannt eingeschätzt, liegt dieser Anteil bezogen auf die aktuelle Situation bei 48 %. Unternehmen mit eher angespannter wirtschaftlicher Situation schätzen die Auswirkungen der Corona-Krise auf die IT-Sicherheit deutlich häufiger negativ ein und treffen seltener zusätzliche IT-Sicherheitsmaßnahmen. Dazu zeigten die Auswertungen, dass die Möglichkeit von Homeoffice im Zusammenhang mit einer höheren Betroffenheitsrate bezüglich Phishing- Angriffen und die Möglichkeit der Nutzung privater Hard- und Software im Zusammenhang mit einer höheren Betroffenheitsrate bezüglich Angriffe mit sonstiger Schadsoftware steht.

IT-Sicherheitsmaßnahmen ermöglichen rechtzeitiges Handeln

Unternehmen, die Risiko- und Schwachstellenanalysen durchführen, gaben deutlich häufiger an, auf mindestens einen Cyberangriff in den letzten zwölf Monaten reagiert zu haben, als Unternehmen ohne diese Maßnahme. Gleichzeitig gab diese Gruppe aber auch deutlich seltener an, einen aus Sicht der Täter*innen (teilweise) erfolgreichen Cyberangriff erlebt zu haben. Dieses und weitere ähnliche Ergebnisse deutet darauf hin, dass die Aufmerksamkeit und die Fähigkeit zur Entdeckung (versuchter)

Cyberangriffe mit vielen IT-Sicherheitsmaßnahmen steigen und damit eine rechtzeitige Reaktion und die Abwehr von Angriffen ermöglicht wird.

Eine Ausnahme bildet die Verschlüsselung von Kommunikation. Unternehmen mit dieser Maßnahme haben seltener auf Cyberangriffe reagiert und seltener (teilweise) erfolgreiche Angriffe erlebt. Mit Verschlüsselung lassen sich demnach sowohl die Angriffsfläche als auch die Erfolgsaussichten für Angreifer*innen reduzieren.

Insgesamt betrachtet ist allerdings davon auszugehen, dass für die Verbesserung der IT-Sicherheit von Unternehmen ein individuell angepasstes Zusammenspiel aus verschiedenen organisatorischen und technischen IT-Sicherheitsmaßnahmen nötig ist, das den sogenannten „Faktor Mensch“ nicht außenvorlässt. Denn beim Großteil der berichteten Cyberangriffe handelte es sich um Phishing-Angriffe, die auf eine Täuschung von IT-Anwender*innen z.B. zur Erlangung sensibler Informationen abzielten. Daneben wurde die Mehrzahl der Angriffe von den Beschäftigten der Unternehmen entdeckt und das häufig auch ohne Beteiligung technischer Maßnahmen. Und viele technische und organisatorische IT-Sicherheitsmaßnahmen können erst eine Wirkung entfalten, wenn diese von den Beschäftigten (richtig) genutzt werden.

Grenzen der Untersuchung

Alle Befragungsstudien unterliegen verschiedenen Einschränkungen, die deren Aussagekraft beeinträchtigen. Hier sind dies im Wesentlichen Unsicherheiten hinsichtlich der Vollständigkeit der Firmendatenbanken aus der die Stichprobe gezogen wurde sowie etwaige Erinnerungs- und Wissenslücken der Befragten, die mit ihren Aussagen jeweils ein Unternehmen repräsentieren. Wie bei anderen Befragungsstudien auch besteht die Möglichkeit, dass die Befragten Antworten gegeben haben, die sich tendenziell eher daran orientierten, wie es sein müsste als daran, wie es ist. Zudem konnten mit dieser Erhebungsmethode keine Informationen zu unbemerkt gebliebenen Cyberangriffen (absolutes Dunkelfeld) gesammelt werden und der Detailgrad der Fragen, z.B. zu Qualität und Reifegraden von IT-Sicherheitsmaßnahmen, war aufgrund zeitlicher Grenzen beschränkt. Hinzu kommt, dass an der Folgebefragung nur ein relativ kleiner Teil der Unternehmen erneut teilgenommen hat

Trotz der genannten Restriktionen, liegen für Deutschland nun erstmals längsschnittliche Dunkelfelddaten zum Thema Cyberangriffe gegen Unternehmen vor, die unabhängig, nach wissenschaftlichen Gütekriterien durchgeführt und transparent dokumentiert wurde. Damit bietet sie eine gute Grundlage für Einschätzungen zu diesem Themenbereich, die weit über die Erkenntnisse anhand von Hellfelddaten wie der Polizeilichen Kriminalstatistik (PKS) hinausgehen und Anknüpfungspunkte für weitere Forschung bieten.

Weitere Analysen sollen u.a. zeigen, wie sich die z.T. große Varianz hinsichtlich des Reifegrads weitverbreiteter IT-Sicherheitsmaßnahmen auf das Angriffsrisiko auswirkt.

Zum KFN

Das Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) ist eine unabhängig und interdisziplinär arbeitende Forschungseinrichtung, welche 1979 gegründet wurde. Es hat die Aufgabe, als selbstständige Forschungseinrichtung praxisorientierte kriminologische Forschung zu betreiben und zu fördern. Träger ist ein gemeinnütziger Verein. Das KFN wird vom Niedersächsischen Ministerium für Wissenschaft und Kultur im Rahmen einer institutionellen Förderung finanziert und betreibt kriminologische Forschung in verschiedenen Themenfeldern.

Weiterführende Informationen finden Sie auf der Webseite des KFN: www.kfn.de

Ansprechpartner*innen zur Studie:

Arne Dreißigacker, Soziologe, KFN,
E-Mail: arne.dreissigacker@kfn.de;
Tel.: +49 (511) 34836-28

Bennet von Skarczinski, Betriebswirt, PwC
E-Mail: bennet.simon.von.skarczinski@pwc.com
Tel.: +49 (511) 34836-29

Prof. Dr. Gina R. Wollinger, Soziologin, HSPV NRW
E-Mail: ginarosa.wollinger@hspv.nrw.de;
Tel.: +49 (221) 912652-3590