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, 16.03.2020**

Cyberangriffe: Unternehmen im Visier

Risiko- und Schutzfaktoren erkennen, IT-Sicherheit erhöhen: KFN veröffentlicht erste Ergebnisse einer großen deutschlandweiten Befragung von 5.000 Unternehmen zum Thema Cyberangriffe

Insgesamt 41 % der Unternehmen ab zehn Beschäftigten in Deutschland erlebten innerhalb eines Jahres mindestens einen Cyberangriff, auf den sie reagieren mussten. Aber nicht alle Unternehmen sind gleichermaßen betroffen. Dies gehört zu den zentralen Ergebnissen einer großangelegten repräsentativen Befragung von 5.000 Unternehmen, welche das Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) am 16.03.2020 vorlegt.

Insbesondere in den Gruppen der kleinen und mittleren Unternehmen musste häufiger auf Cyberangriffe reagiert werden, wenn die Unternehmen mehrere Standorte im In- oder Ausland hatten, Waren oder Dienstleistungen exportierten oder über besondere Produkte, Herstellungsverfahren, Reputationen oder Kundenkreise verfügten. „*Wenn man von solchen Risikofaktoren weiß, können Unternehmen gezielter darin unterstützt werden, ihre IT-Sicherheit zu verbessern*“, sagt der Soziologe Arne Dreißigacker (Leiter der Befragung).

Die Untersuchung ergab zudem, dass technische IT-Sicherheitsmaßnahmen bereits sehr weit verbreitet sind. Maßnahmen, die sich auf die Organisation der Unternehmen beziehen, z.B. IT-Sicherheitsschulungen für Beschäftigte oder schriftlich fixierte Richtlinien zur IT-Sicherheit, werden hingegen seltener eingesetzt. Unternehmen, die nicht nur auf Technik setzen, sind tendenziell seltener von Cyberangriffen betroffen. „*Es wird also in Zukunft darum gehen, IT-Sicherheitsmaßnahmen besser in organisatorische Abläufe und Prozesse der Unternehmen einzubinden und das Zusammenspiel von Mensch und Technik stärker in den Blick zu nehmen*“, schlussfolgert Prof. Dr. Sascha Fahl (Teilprojektleiter, Leibniz Universität Hannover).

Gefördert wird dieses Projekt durch die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (BMWi). Eine Zusatzförderung erfolgt 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. 152, zu dem derzeit eine zusätzliche Kurzversion für Verantwortliche und Entscheider*innen kleiner und mittlerer Unternehmen erarbeitet wird.

Ansprechpartner:

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

Prof. Dr. Sascha Fahl, Informatiker, LUH
E-Mail: fahl@sec.uni-hannover.de;
Tel.: +49 (511) 76214835

Zusatzförderung durch: pwc VHV STIFTUNG

Das Forschungsprojekt „Cyberangriffe gegen Unternehmen“

Das KFN führt zusammen mit dem Forschungszentrum L3S der Universität Hannover von Dezember 2017 bis November 2020 ein umfangreiches Forschungsprojekt zum Thema „Cyberangriffe gegen Unternehmen“ durch. Das Projekt wird 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 wird 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. Die Erkenntnisse aus den einzelnen Untersuchungen werden in einer zweiten Phase des Vorhabens genutzt, um Handlungsempfehlungen zu erstellen und auf unterschiedlichsten Wegen kleinen und mittelständischen Unternehmen zugänglich zu machen.

Methode und Stichprobe der Unternehmensbefragung

Die Befragung der 5.000 Unternehmen wurde per computergestützten Telefoninterviews (CATI) zwischen August 2018 und Januar 2019 durchgeführt. Der eingesetzte standardisierte Fragebogen enthielt 40 Fragen zur Risikoeinschätzung, zu erlebten Cyberangriffen, zu IT-Sicherheitsmaßnahmen, zu Unternehmensmerkmalen, zum Anzeigeverhalten und zum Versicherungsschutz.

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). Neben 1.000 kleinen Unternehmen mit 10-49 Beschäftigten und 3.000 mittleren Unternehmen mit 50-499 Beschäftigten sind auch 500 große Unternehmen ab 500 Beschäftigten als Vergleichsgruppe enthalten. Zusätzlich wurden weitere 500 Unternehmen der Daseinsvorsorge (z.B. Energie- und Wasserversorgung, Gesundheitswesen, Verkehrsbetriebe) einbezogen. 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 im Jahr 2018, womit verallgemeinerbare Aussagen 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 % der gewichteten Stichprobe ausmachen.

Zentrale Ergebnisse der Unternehmensbefragung

Betroffenheit von Cyberangriffen

Über alle Angriffsarten hinweg waren etwa zwei Fünftel der Unternehmen ab 10 Beschäftigten 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 (41 %). 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 (22 %) und Schadsoftwareangriffen (Ransomware: 13 %, Spyware: 11 % und sonstige Schadsoftware: 21 %) betroffen waren, gefolgt von CEO-Fraud (8 %), (D)DoS (6 %), Defacing und manuellem Hacking (jeweils 3 %).

Im Unternehmensgrößenvergleich fallen relativ große Unterschiede bezüglich Ransomware, Phishing und besonders beim CEO-Fraud auf. Große Unternehmen sind von diesen Angriffsarten anteilig deutlich häufiger betroffen als kleine Unternehmen. Neben einer höheren Präsenz im Internet und einer umfangreicheren IT-Infrastruktur wirkt sich wahrscheinlich auch die mit der Unternehmensgröße zunehmende Anonymität unter den Beschäftigten aus.

Weitere signifikante Unterschiede hinsichtlich der Betroffenheit der Unternehmen zeigen sich zwischen verschiedenen Branchen bzw. Wirtschaftszweigen. Unternehmen der Daseinsvorsorge waren z.B. seltener betroffen (31,1 %) als Unternehmen der übrigen Branchen (42,3 %) und scheinen demzufolge tendenziell besser geschützt zu sein oder entgegen der Erwartung weniger angegriffen zu werden.

Risikofaktoren

Große Unternehmen (ab 500 Beschäftigte) mussten anteilig deutlich häufiger auf Cyberangriffe in den letzten zwölf Monaten reagieren (58 %) als kleine Unternehmen (10-49 Beschäftigte: 39 %). Dieser Unterschied relativiert sich jedoch, wenn zusätzlich weitere Unternehmensmerkmale in den Blick genommen werden. Die Betroffenheitsraten innerhalb der Gruppen kleiner und mittlerer Unternehmen sind zum Teil sehr viel höher, wenn sie z.B. mehrere Standorte in Deutschland, mindestens einen zusätzlichen Standort im Ausland haben oder Güter bzw. Dienstleitungen exportieren. Bei Unternehmen, die über besondere Produkte, Herstellungsverfahren etc. oder eine besondere Reputation/ Kundenkreise verfügen, ist der Anteil der Betroffenen ebenfalls deutlich größer als bei den übrigen Unternehmen.

Folgen der schwerwiegendsten Cyberangriffe

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

Bei 70 % der betroffenen Unternehmen entstanden direkte Kosten infolge dieses schwerwiegendsten Angriffes, wobei dieser Anteil bei kleinen Unternehmen (10-49 Beschäftigte: 72 %) etwas höher lag als bei den großen (ab 500 Beschäftigte: 65 %). Bei kleineren Unternehmen entstanden vergleichsweise häufig Kosten durch externe Beratung und die Wiederherstellung und Wiederbeschaffung, da sie in der in der Regel weniger eigene IT- oder sogar IT-Sicherheitsabteilungen haben und daher häufiger Dritte zu Rate ziehen mussten.

Neben den genannten Kostenpositionen wurden insgesamt am häufigsten Kosten für Sofortmaßnahmen zur Abwehr und Aufklärung angeführt (40 %). Von Kosten durch Schadensersatz/ Strafen (1 %) und abgeflossene Gelder (2 %) wurde hingegen relativ selten berichtet.

Die Höhe der direkten Gesamtkosten konnten bei 31 % der Unternehmen, bei denen Kosten entstanden sind, aufgrund fehlender Angaben nicht berechnet werden. Bezogen auf die übrigen Fälle reichten die direkten Gesamtkosten bis zu 2 Mio. Euro, lagen im Durchschnitt bei rund 16.900 Euro und im Median bei 1.000 Euro.

Auch wenn die direkten Kosten im Durchschnitt bzw. im Median erst einmal relativ gering erscheinen, darf nicht vergessen werden, dass sich diese auf jeweils einen Cyberangriff im letzten Jahr beziehen und auch versuchte Angriffe mitumfasst sind, die vereitelt werden konnten. In Hinblick auf die höheren Werte der angegebenen Gesamtkosten können „erfolgreiche“ Cyberangriffe gerade für kleine und mittlere Unternehmen ein bestandsgefährdendes Ausmaß annehmen. Hinzu kommt, dass mögliche indirekte Kosten, wie z.B. Umsatzverluste aufgrund von Imageschäden oder erfolgreicher Produktspionage, die noch Monate nach dem Cyberangriff anfallen können, hier unberücksichtigt bleiben.

Anzeigeverhalten

Bezogen auf den schwerwiegendsten Cyberangriff der letzten zwölf Monate gaben lediglich 12 % der Unternehmen an, diesen polizeilich angezeigt zu haben. Zu den am häufigsten angezeigten Angriffsarten zählen CEO-Fraud (25 %), Spyware (20 %) und manuelles Hacking (19 %). Große Unternehmen (ab 500 Beschäftigte) erstatteten mit 22 % häufiger Anzeige als kleine Unternehmen (10-49 Beschäftigte) mit 11 %. Bemerkenswert ist, dass über ein Fünftel der kleineren Unternehmen als Nichtanzeigegrund angab, gar nicht zu wissen, an wen man sich dafür zu wenden habe. Dies weist auf einen Informationsbedarf hin und bietet einen Ansatzpunkt zur Erhöhung der Anzeigequote. Der häufigste Nichtanzeigegrund ist allerdings die fehlende Aussicht auf einen Ermittlungserfolg (72 %). Befürchtungen von Imageschäden (3 %), Arbeitsbehinderungen (11 %) oder von behördlicher Einsicht in vertrauliche Daten (5 %) spielen demgegenüber nur eine kleinere Rolle.

Schutzfaktoren

Viele der erfragten technischen IT-Sicherheitsmaßnahmen – z.B. regelmäßige Backups und deren physisch getrennte Aufbewahrung, aktuelle Antivirensoftware, regelmäßige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches sowie der Schutz der IT-Systeme mit einer Firewall – wurden von fast allen Unternehmen eingesetzt. Trotzdem waren viele dieser Unternehmen im letzten Jahr von mindestens einem Cyberangriff betroffen. Dieser Umstand weist darauf hin, dass die Wirkung technischer Maßnahmen mit weiteren Faktoren zusammenhängt. Neben der Qualität, dem Reifegrad sowie der sachgemäßen Konfiguration und Wartung der technischen Maßnahmen dürften dazu ebenso die Frage des Designs, der Nutzbarkeit und der Einbindung in organisatorische Abläufe und Prozesse zählen.

Organisatorische IT-Sicherheitsmaßnahmen waren im Vergleich zu den technischen weniger weit verbreitet, standen aber fast alle im Zusammenhang mit der Betroffenheit von Cyberangriffen. Insbesondere Unternehmen, die ihre Richtlinien zur IT-Sicherheit und zum Notfallmanagement regelmäßig überprüfen und Verstöße gegebenenfalls ahnden, waren signifikant seltener in den letzten zwölf Monaten von Cyberangriffen betroffen als Unternehmen, die dies nicht taten. Es kommt also nicht nur darauf an, entsprechende Richtlinien und IT-Sicherheitsmaßnahmen einzuführen, sondern diese auch innerhalb des Unternehmens ‚zu leben'. Nicht vergessen werden darf, dass solche Richtlinien technische Maßnahmen voraussetzen, die sich in den Arbeitsalltag der Beschäftigten gut integrieren lassen sollten.

Schriftlich fixierte Richtlinien zum Notfallmanagement, die Zertifizierung der IT-Sicherheit sowie regelmäßige Risiko- und Schwachstellenanalysen stehen ebenfalls im Zusammenhang mit niedrigeren Betroffenheitsraten. Schulungen zur IT-Sicherheit für Beschäftigte weisen bei mittleren Unternehmen einen Zusammenhang mit einer niedrigeren Betroffenheit aus, während dies bei Mindestanforderungen für Passwörter vor allem bei den kleinen Unternehmen der Fall ist.

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.

Trotz der genannten Restriktionen zählt diese Unternehmensbefragung derzeit zu den größten und aussagekräftigsten Studien zum Thema Cyberangriffe gegen Unternehmen, die unabhängig, nach wissenschaftlichen Gütekriterien durchgeführt und transparent dokumentiert wurde. Damit bietet sie eine gute Grundlage für Einschätzungen zu diesem Themenbereich sowie Anknüpfungspunkte für weitere Forschung.

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.

Zum L3S

Das L3S ist ein Forschungszentrum der Leibniz Universität Hannover und der Technischen Universität Braunschweig für grundlagen- und anwendungsorientierte Forschung im Bereich Web Science und digitale Transformation. L3S-Forscher entwickeln zukunftsweisende Methoden und Technologien, die einen intelligenten, nahtlosen und sicheren Zugriff auf Informationen über das Web ermöglichen, Individuen und Gemeinschaften in allen Bereichen der Wissensgesellschaft vernetzen und das Internet an die reale Welt und ihre Einrichtungen anbinden.

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

Ansprechpartner*innen:

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

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

Prof. Dr. Sascha Fahl, Informatiker, LUH
E-Mail: fahl@sec.uni-hannover.de;
Tel.: +49 (511) 76214835

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