Ergebnisprotokoll

Ausschuss für Unternehmensgründung und -förderung

Sitzung am 30. November 2023, 17.00 bis 19.00 Uhr,
in der Handelskammer, Alster-Zimmer,
Adolphsplatz 1, 20457 Hamburg

Tagesordnung

TOP 1 **Begrüßung**
Carlo Ulbrich, Nect GmbH

TOP 2 **Rückblick auf eine Cyberattacke**
Steve Wendt, Handelskammer Hamburg

TOP 3 **“You have been hacked!” - interaktives Fallbeispiel**
Henry Georges, LKA Hamburg

TOP 4 **Von Risiko zu Sicherheit: Einblicke, Erfahrungen, Lösungen und Kriterien der Versicherbarkeit aus Sicht eines Erstversicherers**
Richard Weber und Cedric Willhoeft, Hiscox SA

TOP 5 **Sonstiges**

Teilnehmer:

Vorsitzender: Herr Ulbrich

Mitglieder: Frau Biehl, Herr Dannies, Frau Gritzuhn, Herr Hartenstein, Frau Horn, Frau Huppmann, Frau Jeschke, Herren Neumann, Rother, Tonne

Gäste: Herr Carsten, Frau Lucius

ReferentInnen: Herr Georges, Herr Wendt, Herr Willhoeft

Hauptamt: Herr Hoops, Frau Kersten, Frau Schroers (Protokoll)

TOP 1 Begrüßung

Herr Ulbrich begrüßt alle Mitglieder des Ausschusses sowie die Referenten der Sitzung im Alster-Zimmer der Handelskammer. Er betont, dass die Tagesordnungen der vergangenen Sitzungen mit Unterstützung aus den Reihen der Mitglieder erstellt worden seien. Das zeige die gute Kooperation von Haupt- und Ehrenamt und führe dazu, dass die Sitzungsthemen besonders gut auf das Interesse der Mitglieder einzahle.

Das Protokoll der Sitzung vom 28. September 2023 wird ohne Änderungen freigegeben.

TOP 2 Rückblick auf eine Cyberattacke

Herr Hoops berichtet, nicht zuletzt auf der Basis der eigenen Erfahrungen aus der Cyber-Attacke im vergangenen Jahr, habe die Handelskammer das Thema Cybersicherheit in ihren Gremien und bei Veranstaltungen für die Mitgliedsunternehmen in diesem Jahr priorisiert. Dazu gehörten u.a. verschiedene Veranstaltungsformate, wie eine Webinar-Reihe, der IT-Sicherheitstag und regelmäßige Cybercrime-Sprechtage. Darüber hinaus gebe es unter www.hk24.de/it-sicherheit eine Landingpage mit Informationen für Unternehmen. Ansprechpartnerin im Hause zu diesem Thema sei Jenny Kersten, die ebenfalls bei der Sitzung anwesend ist. Mit der heutigen Sitzung solle ein Überblick über das Thema geboten und die Frage gestellt werden, welche Bedeutung Cybersicherheit insbesondere für junge Unternehmen und Gründungsvorhaben habe.

Als Einstieg werde Steve Wendt, Leiter der Abteilung „Digital voraus“ unserer Handelskammer über den Sicherheitsvorfall des IHK-Verbunds aus dem August 2023 berichten.

Herr Wendt erläutert, das Infrastrukturnetz der Handelskammer Hamburg als Teil eines IHK-Verbunds mit 79 IHKn, der DIHK sowie Zweigstellen und den Außenhandelskammern, umfasse insgesamt ca. 9.000 User. Alle Standorte seien in einem gemeinsamen IHK-Wan (Weitverkehrsnetz) eingebunden, wodurch es nur einen zentralen Übergangspunkt ins Internet gebe. Der Angriff sei im Mai 2022 über einen Zero Day Exploit auf zwei Wissensdatenbanken erfolgt und bis Ende Juli unentdeckt geblieben. Ziel des hochprofessionellen Angriffs seien die Daten im IHK-Netz gewesen. Nach der Trennung der Systeme vom Internet, seien die Systeme im Notbetrieb aufrechterhalten worden. Stück für Stück hätten der Krisenstab im Verbund mit den IT-Abteilungen der Kammern und ausgewählten IT-Dienstleistern alle Soft- und Hardware-Schnittstellen gehärtet und in einen neuen Regelbetrieb überführt. Damit sei nicht nur die Außerbetriebnahme vieler Geräte, sondern auch der zeitweise der Verzicht auf alle Office-Produkte und Spezialprogramme einhergegangen. Dies habe die Mitarbeiterschaft vor große organisatorische und kommunikative Herausforderungen gestellt. Erst Mitte September sei der Regelbetrieb unter erneuerten und deutlich schärferen Sicherheitsmaßnahmen wieder aufgenommen worden. Im IHK-Verbund werde jetzt an einem gemeinsamen Sicherheits-Standard, vorsorgenden Maßnahmen und an einem auf den Erfahrungen aufbauenden Notfallplan gearbeitet. Ein Zero Trust Ansatz werde geprüft, führe jedoch zum Teil zu erheblichen Eingriffen in die Arbeitsprozesse.

Auf Nachfrage berichtet Herr Wendt, dass der Faktor „Mensch“ immer die größte Sicherheitslücke darstelle, die die Handelskammer versuche, mit Awareness-Trainings zu schließen. Die Angriffe per Mail seien jedoch zum Teil so authentisch, dass falsche Reaktionen im Umgang mit Angriffsversuchen nie ganz zu verhindern seien.

TOP 3 “You have been hacked” – interaktives Fallbeispiel

Henry Georges stellt sich als Berater der Hamburger Zentralen Ansprechstelle Cybercrime (ZAC) des LKA vor. Die Dienststelle sei seit 2019 mit fünf Ermittlern für Krypto-Ermittlungen sowie für die Beratung von Unternehmen zuständig. Zu den Beratungsangeboten gehörten Awareness-Schulungen, Übungen sowie Hilfe bei der Erstellung von Notfallplänen. Im Rahmen eines interaktiven Vortags führt Herr Georges durch die entscheidenden Situationen eines Cyber-Angriffs und gibt Hinweise, wie Unternehmen sich schon im Vorfeld wappnen können, um einem Angriff so zu begegnen, dass ein möglichst geringer Schaden entsteht.
Auf Nachfrage, warum die Dienststelle trotz der großen Bedrohung mit so wenigen Personen ausgestattet sein, erläutert Herr Georges, dass es u.a. schwer sei, geeignetes Personal zu finden, da auch auf diesem Bereich ein Fachkräftemangel bestehe.
Er führt weiter aus, im Fall eines Sicherheitsvorfalls sei es für die Unternehmen notwendig, neben der Polizei auch IT-Dienstleister ins Boot zu holen. Diese unterstützen bei der Aufklärung des Vorfalls aber auch an der Widerherstellung der Systeme. Kurzfristig seien auch die z.T. schwer zu bekommen, weshalb sich u.U. die Investition in eine Cyber-Versicherung lohne, da dort Dienstleister zur Verfügung gestellt würden. Herr Georges macht deutlich, dass auch bei der Nutzung von Cloud-Diensten das Unternehmen Sorge tragen müsste, ein Backup- und Sicherheits-System aufzubauen. Da die Zeitspanne zwischen Angriffen und Erpressungsversuchen immer größer würden, sei es zum Teil schwierig, ein Backup-System zu erstellen, dass auch auf diese großen Zeiträume reagiere. Wichtigste Botschaft der ZAC sei, das Personal regelmäßig zu schulen, Notfallpläne zu entwickeln und einen Krisenstab zu erstellen, der im Notfall frei Hand bei der Umsetzung von Maßnahme habe, damit keine wertvolle Zeit verloren gehe. Die Frage, ob ein Unternehmen Lösegeld zahlen solle, sei individuell abzuwägen. Lösegeld zu zahlen hieße nicht immer, dass alle Daten einwandfrei wiederhergestellt werden könnten.

TOP 4 Von Risiko zu Sicherheit: Einblicke, Erfahrungen, Lösungen und Kriterien der Versicherbarkeit aus Sicht eines Erstversicherers

Herr Willhoeft, Underwriter Commercial Lines der Hamburger Niederlassung von Hiscox SA, erläutert in seinem Vortrag die allgemeinen Trends zum Thema Cybersicherheit, geht auf die aktuelle Risikolage ein und macht deutlich, welche Bedingungen Unternehmen erfüllen müssen, um von einem Cyberversicherer versichert zu werden. Hiscox sei der erste Versicherer gewesen, der im Jahr 2011 in Deutschland eine Deckung für Cyber- und Datenrisiken angeboten habe. Die Versicherung umfasse auch präventive Maßnahmen und Soforthilfe im Schadensfall. Eine Umfrage der Hiscox habe gezeigt, dass ein Angriff die Unternehmen durchschnittlich etwa 16.000 Euro koste, die teuersten Attacken hätten sich in den vergangenen Jahren auf 3.400.000 Euro belaufen. Die Schadenshäufigkeit pro Vertrag steige nahezu exponentiell. Den größten Teil der angegriffenen Unternehmen machten mit 36% kleine Unternehmen mit bis zu 10 Mitarbeitenden aus. Die Kompromittierung von Geschäfts-E-Mails sei der beliebteste Einstieg der Hacker (35 %), gefolgt vom Hack über einen Unternehmens- oder Cloud-Server (31%).

Ein Cyberversicherer übernehme im Schadensfall beispielsweise Kosten für Krisenmanagement, IT-Forensik, Rechtsberatung, PR-Maßnahmen, Wiederherstellungskosten, Lösegelder etc. Dabei sei die Fahrlässigkeit generell versichert, jedoch müssten Unternehmen vor Vertragsabschluss das eigene Sicherheitskonzept ausführlich darlegen. Sollte ein Sicherheitskonzept fehlen oder unzureichend sein, gebe es nur wenig Chance auf einen Versicherungsschutz.

Der Ausschuss diskutiert im Anschluss, inwiefern es sinnvoll sein könnte, gerade junge Unternehmen und Gründende auf diese Gefahren hinzuweisen und schon im Gründungsprozess ein Sicherheitskonzept abzufordern. Herr Hoops bietet an, das Thema Cyber-Security über die

Mediathek der Unternehmenswerkstatt Deutschland noch stärker in den Fokus zu nehmen und Informationen über Webinar-Inhalte zur Verfügung zu stellen, damit Gründende ausreichend informiert würden.

TOP 5 Sonstiges

Herr Ulbrich nennt den Termin der letzten Sitzung der Wahlperiode, Do. 14.03.2024, 17 - 19 Uhr. Er schließt die Sitzung um 19.15 Uhr und bedankt sich für das Erscheinen und lädt zum anschließenden Après auf dem Weihnachtsmarkt.

30.11.2023

Gez. Carlo Ulbrich