LÜNENDONK

PRESSEINFORMATION

IT-07-04-22

CYBER SECURITY: BEDROHUNGSLAGE UND AUCH DIE INVESTITIONEN NEHMEN ZU

- **Finanzdienstleister schätzen das Risiko von Cyber-Angriffen als hoch ein, fühlen sich aber gut vorbereitet**
- **Ransomware, Phishing und DDos-Attacken werden als größte Gefahren eingestuft**
- **Große Sorge besteht um Abfluss von Kundendaten, Imageschäden und Lösegeldforderungen**
- **Budgets für Cyber Security werden 2022 und 2023 stark steigen**
- **Neue Lünendonk-Studie ab sofort kostenfrei verfügbar**

Mindelheim, 07. April 2022 – Finanzdienstleister sind sich der Gefahr schwerwiegender Cyber-Angriffe zwar bewusst, fühlen sich aber gleichzeitig gut vorbereitet, diese frühzeitig zu erkennen und abzuwehren. Eine deutliche Mehrheit der Banken, Versicherungen und Vermögensverwalter verfolgt eine klare Cloud-Strategie und verspricht sich ein höheres Sicherheitsniveau durch die Nutzung von Cloud-Diensten. Allerdings erkennt man gleichzeitig auch die Notwendigkeit, mehr in IT Security zu investieren.

Dies sind ausgewählte Ergebnisse der neuen Lünendonk-Studie 2022 „Von Cyber Security zur Cyber Resilience – wie Finanzdienstleister auf die neue Bedrohungslage reagieren", die in Zusammenarbeit mit KPMG erstellt wurde.

Digitalisierung eröffnet Hackern neue Angriffsmöglichkeiten

92 Prozent der Finanzdienstleister sehen ihr Unternehmen gut gegen Cyber-Angriffe geschützt. Ebenso stimmen 87 Prozent der Aussage voll oder

überwiegend zu, dass IT Security als Wertschöpfungsfaktor und fester Bestandteil der digitalen Transformation gesehen wird. „Durch den steigenden Digitalisierungsgrad – vor allem an den Kundenschnittstellen im Frontend – entstehen neue Einfallstore und eine größere Angriffsfläche für Hacker, die es schnell zu schließen gilt. Daher überrascht es, dass viele der Studienteilnehmenden ihre Unternehmen als gut gegen Cyber-Angriffe aufgestellt sehen", erläutert Mario Zillmann, Partner bei Lünendonk und Autor der Studie. Christian Nern, Partner bei KPMG ergänzt: „Aus regulatorischer Sicht wurde zwar prozessseitig in den letzten Jahren viel für eine bessere IT Security geleistet. Aus der IT-/Cyber-Security-Sicht betrachtet, fehlt es den meisten Financial-Services-Instituten aber an einer unternehmensweiten Security-Architektur beziehungsweise geeigneten Security-Maßnahmen hinsichtlich einer veränderten digitalen Welt mit Cloud, Apps und Plattformen. Auch für eine bessere Mitarbeiter-Awareness gegenüber Phishing-Kampagnen oder Automatisierung und Integration einzelner IT-Security-Systeme muss mehr gemacht werden."

Als größte Cyber-Bedrohung sehen 68 Prozent der befragten Banken, Versicherungen und Vermögensverwaltungen Ransomware und Phishing-Mails, gefolgt von der Nutzung unautorisierter Devices (66 %). 55 Prozent halten es ebenso für wahrscheinlich, Opfer einer DDos-Attacke (Distributed-Denial-of-Service) zu werden, die Dienste oder Webseiten blockieren und unbenutzbar machen. „Die Methoden und Technologien, die für Cyber-Attacken genutzt werden, sind vielfältig und entwickeln sich ständig weiter. Hacker sind in der Regel ihren Zielen zwei Schritte voraus und häufig schon lange vor dem tatsächlichen Angriff bereits in den IT-Systemen. Gerade deshalb gilt es, in das Identifizieren von Schwachstellen und die Prävention von Cyber-Angriffen zu investieren", schätzt Zillmann die Situation ein. „Dabei kommt es aber nicht nur auf prozessuale und technologische Aspekte an,

sondern vor allem auf die Sensibilisierung der Mitarbeitenden gegenüber Angriffsversuchen, beispielsweise via Phishing-Kampagnen.
Als häufigste Folge von Cyber-Attacken sehen 73 Prozent der Finanzdienstleister einen Abfluss von Kundendaten. 67 Prozent befürchten den Abgriff kritischer Unternehmensdaten. Hohe Lösegeldforderungen (33 %) oder Umsatzeinbußen (31 %) erwartet jeder dritte Studienteilnehmende.

Budgets für Cyber Security sollen steigen

Um den Schutz der IT- und Unternehmenssysteme zu erhöhen, sollen die Ausgaben für IT Security teilweise sehr stark steigen. Während für Detection, Response und Recovery, also Aktivitäten nach einem erfolgten Angriff, die Budgets vorwiegend um bis zu 10 Prozent steigen oder konstant bleiben sollen, wird in den Bereichen Identify und Prevention, also der frühzeitigen Erkennung von Schwachstellen und Abwehr von Angriffen, von deutlich stärkeren Budgeterhöhungen ausgegangen.

Über die Lünendonk-Studie

Für die Lünendonk-Studie 2022 „Von Cyber Security zur Cyber Resilience – wie Finanzdienstleister auf die neue Bedrohungslage reagieren" wurden 100 Führungskräfte – vornehmlich aus der IT – von Banken, Versicherungen und Vermögensverwaltungen aus dem gehobenen Mittelstand sowie aus Großunternehmen und Konzernen befragt. Die Studie gibt ein Bild zur Wahrnehmung von Cyber-Attacken und welche Strategien für mehr Cyber-Sicherheit verfolgt werden. Sie wurde in fachlicher Zusammenarbeit mit KPMG realisiert und steht unter www.luenendonk.de zum kostenlosen Download zur Verfügung.

Unternehmensprofil
Lünendonk: Informationen zur Orientierung

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Management- und IT-Beratung, Wirtschaftsprüfung, Steuer- und Rechtsberatung, Facility Management und Instandhaltung sowie Personaldienstleistung (Zeitarbeit, Staffing).

Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden „Lünendonk-Listen und -Studien" heraus.

Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Unternehmer mit den Lünendonk-Service-Awards aus.

Weitere Informationen

Lünendonk & Hossenfelder GmbH
Mario Zillmann
Partner
Telefon: +49 8261 73140-0
E-Mail: zillmann@luenendonk.de

vibrio. Kommunikationsmanagement
Sascha Smid
Senior PR-Berater
Telefon: +49 89 3215170
E-Mail: luenendonk@vibrio.de

Lünendonk & Hossenfelder GmbH

Maximilianstraße 40, 87719 Mindelheim
Telefon: +49 8261 73140-0 Telefax: +49 8261 73140-66
Homepage: https://www.luenendonk.de

vibrio. Kommunikationsmanagement Dr. Kausch GmbH

Rundfunkplatz 2, 80335 München
Telefon: +49 89 3215170
Homepage: https://vibrio.eu/

Diese Presseinformation und die Grafiken finden Sie im Internet unter:
https://www.luenendonk.de/presseinformationen/