

PRESSEINFORMATION

IT-31-05-23

NEUE LÜNENDONK-STUDIE ZU CYBER SECURITY 2023: DIE BEDROHUNGSLAGE STEIGT WEITER AN

- **Cyber-Bedrohung nimmt im Jahr 2023 weiter zu**
- **Security-Prozesse hinken den Anforderungen an Digitalisierung und Cloud-Nutzung hinterher**
- **Investitionen in Cyber Security steigen weiter**
- **Neue Lünendonk-Studie ab sofort kostenfrei verfügbar**

Mindelheim, 31. Mai 2023 – Die Gefahr, Opfer eines Cyber-Angriffs zu werden, ist im vergangenen Jahr nochmals gestiegen. Infolge der voranschreitenden Digitalisierung ergeben sich neue Einfallstore und Angriffsvektoren für Hacker. Ebenso sind die Verschlüsselung und der Verkauf digitaler Assets und sensibler Daten ein lukratives Geschäft für Cyber-Angriffe. 84 Prozent der Unternehmen stufen folglich für das Jahr 2023 die Gefahrenlage im Vergleich zu 2022 als höher ein. Vor allem die Gefahr von DDoS-Angriffen (Distributed Denial of Service) wird größer eingeschätzt, was unter anderem mit der gestiegenen Professionalität von Hackerorganisationen zusammenhängt. Die Mehrheit der Unternehmen sieht sich zum aktuellen Zeitpunkt jedoch gut auf Cyber-Angriffe vorbereitet, allerdings haben viele Unternehmen auf dem Weg zu einer hohen Cyber-Resilienz noch einige Herausforderungen zu lösen: So beschränken 40 Prozent ihre Cyber-Security-Maßnahmen ausschließlich auf ihre eigenen Unternehmensnetzwerke, anstatt den Blick stärker auf die unternehmensübergreifenden Prozesse zu richten.

Dies sind Ergebnisse der neuen Lünendonk-Studie 2023 „Von Cyber Security

zu Cyber Resilience – Wie Unternehmen auf die steigende Bedrohungslage reagieren“. Die Studie entstand in fachlicher Zusammenarbeit mit KPMG und steht ab sofort unter www.luenendonk.de zum kostenfreien Download bereit.

Cyber Security wird essenziell und komplexer

Mit zunehmender Digitalisierung ist es nicht mehr ausreichend, den Fokus nur auf den Schutz der eigenen Unternehmensnetzwerke zu richten. Cyber Security muss frühzeitig bei der Entwicklung von Digitalstrategien und digitalen Produkten berücksichtigt werden. Tatsächlich sehen 86 Prozent der Unternehmen IT-Security bereits als Wertschöpfungsfaktor und festen Bestandteil ihrer Digitalen Transformation an.

„Die Ergebnisse zeigen, dass die Bedeutung von Cyber Security in Unternehmen im Bewusstsein des Top-Managements angekommen ist. Treiber hierfür sind unter anderem die regulatorischen Anforderungen an den Schutz von Kundendaten und geistigem Eigentum sowie die Absicherung kritischer Infrastrukturen. Allerdings haben viele Unternehmen noch nicht die organisatorische und kulturelle Reife für eine Cyber-Resilienz aufgebaut“, kommentiert Mario Zillmann, Partner bei Lünendonk & Hossenfelder und Studienautor.

Tatsächlich verfügen nur 36 Prozent der befragten Unternehmen über ein zentrales Security Monitoring und nur jedes vierte Unternehmen (25 %) über teil- oder vollautomatisierte Prozesse zur Erkennung und Abwehr von Cyber-Angriffen. Eine zentrale Einheit zur kontinuierlichen Überwachung des Security Monitorings und zur Reaktion auf Vorfälle, haben sogar nur 16 Prozent der befragten Unternehmen aufgebaut.

Aber auch die voranschreitende Cloud-Transformation verändert den Blick auf Cyber Security. „Die Komplexität zur Erkennung und Abwehr von Cyber-Angriffen nimmt durch die Cloud zu“, ergänzt Tobias Ganowski, Consultant bei Lünendonk & Hossenfelder. „Gerade Multi- und Hybrid-Cloud-Landschaften erfordern eine Orchestrierung und Verzahnung der einzelnen Security-Prozesse zu einem integrierten Security-Ansatz. Unternehmen werden daher in den nächsten Jahren die Vernetzung der vielen bereits vorhandenen dezentralen IT-Security-Tools zu integrierten Cloud Security Tool Suites im Sinne eines End-to-End-Managements vorantreiben, ebenso wie die Integration der hybriden Multi-Cloud- und Multi-Provider-Umgebungen in die bestehenden Security-Systeme.“

Cyber-Security-Budgets steigen

„Die meisten Unternehmen haben erkannt, dass nicht die Frage ist, ob, sondern wann sie erfolgreich gehackt werden. Eine hohe Cyber-Resilienz wird somit dadurch erreicht, dass Unternehmen zu jeder Zeit – sei es vor, während oder nach einem Angriff – Transparenz über ihre IT-Systeme haben und wissen, welche Maßnahmen zu welchem Zeitpunkt zu ergreifen sind“, erläutert Mario Zillmann. Daher planen 92 Prozent der befragten Unternehmen für 2023 und 2024 deutlich höhere Investitionen in das Security Monitoring sowie 80 Prozent im Bereich Security Incident and Event Management (SIEM).

Ebenso stehen Cloud Security und Data Center Security nun bei deutlich mehr Unternehmen im Fokus. 69 Prozent werden bis 2024 in Cloud Security investieren (2022: 64 %) und sogar 78 Prozent in Data Center Security (2022: 74 %). Eine weitere Top-Maßnahme ist für 86 Prozent das Vulnerability Management, also Lösungen zur Erkennung von Schwachstellen in den Security-Prozessen.

Über die Lünendonk-Studie

Für die Lünendonk-Studie 2023 „Von Cyber Security zu Cyber Resilience – Wie Unternehmen auf die steigende Bedrohungslage reagieren“ wurden 100 IT- und IT-Security-Verantwortliche mittelständischer Unternehmen und Konzerne befragt. Die Befragten stammen je zur Hälfte einerseits aus dem Finanzsektor sowie andererseits aus Unternehmen in der Industrie, dem Automotive-Bereich, dem Handel, der Energie- und Telko-Branche. Die Studie wurde in fachlicher Zusammenarbeit mit KPMG realisiert und steht ab sofort unter www.luenendonk.de zum kostenfreien Download bereit.

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 Digital & IT, Managementberatung, Wirtschaftsprüfung sowie Steuer- und Rechtsberatung, Real Estate Services und Personaldienstleistung (Zeitarbeit, IT-Workforce).

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 Journalistinnen und Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Persönlichkeiten mit den Lünendonk B2B Service-Awards aus.

Weitere Informationen

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

vibrio. Kommunikationsmanagement
Dorothee Bader
Senior PR-Beraterin
Telefon: +49 89 3215170
E-Mail: lunenendok@vibrio.de

Lünendonk & Hossenfelder GmbH

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