Pressemitteilung **18. Oktober 2023**

Studie „Cybersicherheit in Supply Chains“ von BVL und secida:

Supply Chains in Deutschland sind nicht genug abgesichert – Management nimmt seine Rolle in der Cybersicherheit nur unzureichend wahr

Die unternehmensübergreifende Absicherung von Lieferketten gegen Cyberangriffe ist bislang nur ein Randthema für die meisten Unternehmen. Lediglich 42 % der Unternehmen geben an, Cybersicherheit bereits für die gesamte Supply Chain zu betrachten, insbesondere kleine und besonders große Unternehmen haben hier noch keinen Überblick. Diese sind auch selbstkritisch und konstatieren, dass der Schutz ihrer eigenen Materialflüsse gegen Cyberangriffe nicht zufriedenstellend ist.
Gleichzeitig vertraut das Management vieler Unternehmen auf die Lösungsfähigkeit ihrer IT und nimmt ihre eigene Rolle in der Cybersicherheit nur unzureichend wahr.
Dies sind Erkenntnisse einer neuen Studie, die von der BVL in Zusammenarbeit mit der Universität der Bundeswehr München, der Otto-von-Guericke-Universität Magdeburg sowie den Unternehmenspartnern One Identity, Schunck Group und secida erstellt wurde. In diesem Rahmen wurde eine Befragung von über 150 Mitgliedsunternehmen der BVL durchgeführt.

Deutlich geworden ist, dass Cyberangriffe zu einer Alltagskriminalität geworden sind – fast die Hälfte der befragten Unternehmen wurde in den letzten fünf Jahren mindestens einmal Opfer von Cyberkriminellen, etwa ein Drittel war mehrfach betroffen. Häufig waren Webseiten (30 %) und sensible Daten (25 %) das Ziel, auch Datenverschlüsselung mit anschließender Erpressung kam häufig vor (15 %). Bei der Analyse der Angriffsfälle hat sich herausgestellt, dass vielfach Beschäftigte in den Unternehmen dazu gebracht wurden, Schadsoftware zu installieren (37 %). Auch aus dem Internet zugängliche Schwachstellen waren ein Einfallstor (28 %). Benutzerkennungen und Passwörter wurden in 15 % der Fälle missbraucht.

Nach einem Cyberangriff reagieren die befragten Unternehmen in der Regel professionell. 98 % verbesserten ihre technischen Maßnahmen, 83 % verstärkten Mitarbeiterschulungen, 66 % veränderten ihre Richtlinien und immerhin 48 % stellten zusätzliches Fachpersonal ein.

Die Auswirkungen von Cyberangriffen sind dennoch dramatisch: Fast die Hälfte der Befragten (49 %) gab an, dass die Wiederherstellung der Betriebsfähigkeit nach einem Cyberangriff mehrere Tage oder länger gedauert hat, bei 24 % waren es sogar mehrere Wochen, Monate oder über ein Jahr. Insbesondere bei kleinen Unternehmen mit wenig Kompetenz in der Cybersicherheit oder bei sehr großen Unternehmen mit komplexer IT-Landschaft dauert es lange, bis wieder gearbeitet werden kann.
Dass das Management vieler Unternehmen seine Rolle beim Thema Cybersicherheit noch nicht ausreichend wahrnimmt, verdeutlichen einige Antworten. Obwohl eine Zugehörigkeit zur gesetzlich regulierten kritischen Infrastruktur deutlich höhere

Anforderungen an das Management von Cyberrisiken stellt, kann ein Viertel der befragten Manager nicht sagen, ob das eigene Unternehmen zur kritischen Infrastruktur gehört. Über 40 % der Manager konnten nicht sagen, ob das Unternehmen gegen Cyberangriffe versichert ist oder nicht. 28 % der Befragten wissen nicht, ob das Unternehmen in den letzten fünf Jahren Opfer von Cyberangriffen wurde, 18 % wissen nicht, ob das Risikomanagement im Unternehmen IT-Risiken mitberücksichtigt. Nur jeweils ein gutes Drittel der Unternehmen steuert die Cybersicherheit über entsprechende KPIs oder führt Cybersicherheitsübungen durch.
Wenig überraschend ist, dass kleinere Unternehmen meist weniger der verfügbaren Schutzmaßnahmen gegen Cyberangriffe nutzen, als größere Unternehmen – dabei können Angriffe bei ihnen schneller existenzbedrohend sein.

„In Summe besteht in den Führungsetagen vieler Unternehmen noch großer Nachholbedarf. Die Verantwortung für das Management von Cyberrisiken kann nicht vollständig delegiert werden“, erklärt Alpha B. Barry, CEO der secida AG.

Es gibt aber auch positive Botschaften: die in der Cybersicherheit führenden Unternehmen wurden in den letzten fünf Jahren deutlich häufiger gar nicht gehackt als andere Unternehmen (42% vs. 26%). Die Investition in eine bessere Cybersicherheits-Performance zahlt sich also aus.

„Die Ergebnisse der Studie zeigen sehr klar, dass sowohl das Management vieler Unternehmen, aber auch alle Mitarbeitenden noch mehr für das Thema Cybersicherheit sensibilisiert werden müssen. Als BVL möchten wir dazu beitragen, dass die Unternehmen unseres Wirtschaftsbereichs dabei verstärkt die gesamte Supply Chain in den Blick nehmen“, so der BVL-Vorstandsvorsitzende Prof. Dr.-Ing. Thomas Wimmer.

Programmhinweis:

Die Studienergebnisse werden am
Donnerstag. 19.10. in einer Fachsequenz von 14-14:45 Uhr
im Raum Charlottenburg diskutiert. Auf dem Podium sprechen neben **Alpha Barry** von secida auch **Prof. Dr. Gabi Dreo Rodosek**, Inhaberin des Lehrstuhls für Kommunikationssysteme und Netzsicherheit an der Universität der Bundeswehr in München sowie **Sami Awad-Hartmann**, CIO/International Executive Board bei Hellmann.

Pressekontakt:

Christian Stamerjohanns, Leiter Presse- und Öffentlichkeitsarbeit
Tel.: 0421 173 84 21, Mail: stamerjohanns@bvl.de

Die 1978 gegründete Bundesvereinigung Logistik (BVL) e.V. ist eine gemeinnützige, neutrale und überwiegend ehrenamtliche Organisation. Als Plattform für Manager der Logistik in Industrie, Handel und Dienstleistung, für Wissenschaftler und Studierende bildet sie mit heute rund 10.500 Mitgliedern eine Brücke zwischen Wirtschaft und Wissenschaft und ist Podium für den nationalen und internationalen Gedankenaustausch zwischen Führungskräften aus Logistik und Supply Chain Management.
Mehr unter www.bvl.de