IT- und Sicherheitsexperten zeichnen besorgniserregendes Bild für Europa und die Welt

Die Ergebnisse zeigen, dass fast ein Viertel der Unternehmen nicht auf die Gefahren des Cyberkrieges vorbereitet ist.

GERMANY, January 24, 2023 /EINPresswire.com/ -- Armis, das führende Asset Visibility und IT-Security Unternehmen, gibt die vorläufigen Ergebnisse der „State of Cyberwarfare 2022"-Studie bekannt, die die Stimmung von IT- und Sicherheitsexperten weltweit zum Thema Cyber-Kriegsführung beleuchtet. Die Studie enthält Antworten von mehr als 6.000 Fachleuten aus verschiedenen Branchen, darunter Gesundheitswesen, kritische Infrastruktur, Einzelhandel und Logistik.

Die russische Invasion der Ukraine hat das Leben in dem souveränen Land auf den Kopf gestellt. Zudem werden die geopolitischen Schockwellen, ausgelöst durch die Cyber-Kriegsführung noch auf absehbare Zeit nachhallen. Die Angreifer zielen dabei nicht nur auf die höheren Ebenen der Oppositionsregierungen ab; vielmehr ist jede Organisation ein potenzielles Opfer, wobei kritische Infrastrukturen und sicherheitsrelevante Einrichtungen ganz oben auf der Liste stehen.

„Cyber-Kriegsführung ist die Zukunft des Terrorismus und bietet eine kosteneffektive und asymmetrische Angriffsmethode, die ständige Wachsamkeit und Ausgaben zur Verteidigung erfordert", sagt Nadir Izrael, CTO und Mitbegründer von Armis. „Verdeckte Cyber-Kriegsführung gehört bald der Vergangenheit an. Wir sehen jetzt dreiste Cyberangriffe von Nationalstaaten, oft mit der Absicht, Informationen zu sammeln, den Betrieb zu stören oder Daten zu zerstören. In Anbetracht dieser Trends sollten sich alle Organisationen als mögliche Ziele von Cyberangriffen betrachten und ihre Anlagen entsprechend absichern."

Zu den Schlüsselergebnissen der „State of Cyberwarfare 2022"-Studie gehören:

· Mehr als ein Drittel (33 Prozent) der globalen Organisationen nimmt die Bedrohung durch Cyber-Kriegsführung nicht ernst und ist unbesorgt, was die Auswirkungen auf ihre Organisation als Ganzes betrifft. Diese Einstellung ist bedenklich und provoziert Sicherheitslücken.

· Fast ein Viertel der befragten Unternehmen weltweit (24 Prozent) fühlt sich nicht ausreichend auf den Umgang mit Cyberkriegen vorbereitet. Dennoch genießt nur bei 22 Prozent die Verhinderung von Angriffen durch Nationalstaaten die oberste Priorität ihrer Cybersicherheit.

· Fast zwei Drittel (64 Prozent) der Befragten sind der Meinung, dass der Krieg in der Ukraine eine größere Bedrohung durch Cyber-Kriegsführung zur Folge hat.
· Mehr als die Hälfte (54 Prozent) der Entscheidungsträger für die IT-Sicherheit und 40 Prozent der Befragten auf C-Level (CTO, CIO und CISO) gaben an, dass sie in den letzten sechs Monaten (April-Oktober 2022) mehr Bedrohungsaktivitäten in ihrem Netzwerk erlebt haben als in den sechs Monaten davor.

DACH-spezifische Ergebnisse der Studie
· Die Hälfte der Befragten hat eine Cyberversicherung, die Cyber-Kriegsführung abdeckt. Rund ein Drittel hat noch keine solche Police, plant aber eine abzuschließen.
· Die Teilnehmer wurden zu ihrer Haltung gegenüber Sicherheitsstandards (B3S, IT-Sec 2.0, etc.) befragt. Gut die Hälfte in Deutschland (54 Prozent) sind dabei, zusätzliche Maßnahmen zu ergreifen, um die Situation zu bewältigen. Weniger als ein Drittel sieht sich komplett gerüstet, was die Einhaltung der Richtlinien betrifft.

„Immer mehr deutsche Unternehmen und Organisationen, die als Betreiber von KRITIS im IT-Sicherheitsgesetz 2.0 definiert werden, implementieren die Anforderungen der B3S“, erklärt Mirko Bülles, Director Technical Account Management EMEA bei Armis. „Wie bei jeder Cybersecurity-Strategie muss zunächst eine Inventarisierung aller Assets erfolgen, um danach eine Bewertung vornehmen zu können, welche dieser Assets als besonders schützenswert einzustufen sind. Können die Assets nicht fehlerfrei klassifiziert werden, drohen empfindliche Strafen.“

Weitere Informationen über die „State of Cyberwarfare 2022“-Studie, einschließlich des vollständigen Berichts finden Sie unter: https://www.armis.com/cyberwarfare/

Methodik
Es wurden 6.021 IT- und Sicherheitsexperten in Unternehmen mit mehr als hundert Mitarbeitern befragt – in Großbritannien, den USA, Spanien, Portugal, Frankreich, Italien, Deutschland, Österreich, der Schweiz, Australien, Singapur, Japan, den Niederlanden und Dänemark. Die Ergebnisse wurden zwischen dem 22. September 2022 und dem 5. Oktober 2022 erhoben und zeigen den Stand der Cyber-Kriegsführung weltweit in verschiedenen Regionen und Branchen.

Über Armis
Armis ist die führende Unified Asset Visibility- und Security-Plattform, entwickelt für die neue Bedrohungslandschaft vernetzter Geräte. Fortune-100-Unternehmen vertrauen auf unseren kontinuierlichen Schutz in Echtzeit, um alle verwalteten und nicht verwalteten Assets in den Bereichen IT, Cloud, IoT-Geräte, medizinische Geräte (IoMT), Betriebstechnologie (OT), industrielle Kontrollsysteme (ICS) und 5G mit vollem Kontext zu sehen. Armis bietet passives und unvergleichliches Cybersecurity Asset Management, Risikomanagement und automatisierte Durchsetzung. Armis ist ein privates Unternehmen mit Hauptsitz in Palo Alto, Kalifornien.

Armis

Kafka Kommunikation
armis@kafka-kommunikation.de
Visit us on social media:
Facebook
Twitter
LinkedIn
Other
