Pressemitteilung

Studie zu Cyberattacken: Wie reagierten Unternehmen 2023, und was planen sie 2024?

München, 25. Januar 2024 – Die Software-Bewertungsplattform Capterra veröffentlicht eine Studie zur IT-Sicherheit und zeigt, wie sich die Lage der Cyberbedrohungen im Jahr 2023 entwickelte. Im Rahmen der Studie wurden 1.314 Mitarbeitende dazu befragt, wie Unternehmen auf Cyberbedrohungen reagieren und wie sie ihre Abwehrfähigkeit stärken.

KI-gestützte Angriffe und E-Mail-Phishing-Angriffe stehen ganz oben

Bedrohungen durch KI-gestützte Angriffe (47 %) und neue Methoden von E-Mail-Phishing (46 %) bereiten Unternehmen die meisten Sorgen. Außerdem werden interne Angriffe (25 %), hochentwickelte Ransomware-Angriffe (25 %) und die Kompromittierung geschäftlicher E-Mails (23 %) genannt. Unternehmen sollten auch interne Risiken wie beispielsweise unbeabsichtigtes oder böswilliges Handeln von Partnern oder Mitarbeitenden ernst nehmen.

52 % der Unternehmen bestätigen höhere Ausgaben für die IT-Sicherheit im Jahr 2023

Die wachsende Sorge lässt Unternehmen vor allem in Maßnahmen wie formelle Cybersicherheitsrisikoprüfungen (40 %) und Datenklassifizierung (39 %) investieren. So werden Sicherheitsrisiken oft systematisch bewertet und Daten nach ihrer Sensibilität eingestuft. Weiter setzen Unternehmen auf Zero-Trust-Netzwerksicherheit (31 %), Privileged Access Management (PAM, 28 %) und Netzsegmentierung (27 %), um ihre Infrastruktur zu sichern und den Zugriff auf sensible Bereiche zu kontrollieren.

Bei 42 % der Unternehmen sind die Ausgaben im Vergleich zum Vorjahr gleichgeblieben und 5 % ergriffen keine spezifischen Sicherheitsmaßnahmen. Daraus lässt sich schließen, dass es nach wie vor noch ungeschützte Unternehmen gibt.

Die Top 3 Datenverletzungen

Versehentlich ungesicherte Datenbanken oder Online-Datenquellen machen 42 % der Vorfälle aus. Das zeigt, dass der Umgang mit Daten und deren Sicherung auch 2024 eine Herausforderung für Unternehmen bleibt. Zugleich benennen 42 % böswillige Zugriffe auf Unternehmenssysteme durch Hacker oder andere externe Personen. Bei 20 % der Fälle ist der Diebstahl von Unternehmensdaten durch Mitarbeitende oder andere Insider ein weiterer signifikanter Faktor.

Phishing zeigt hohe Erfolgsrate für Cyberangriffe

Trotz des bestehenden Bewusstseins für Phishing-Mails, aktiven Schulungen und Test-Phishing-Kampagnen seitens der Unternehmen ist die Erfolgsquote von Angriffen noch immer beträchtlich hoch.
8 % der Befragten, die Phishing-Mails erhalten haben, klickten selbst auf bösartige Links.
13 % berichten, dass sowohl sie selbst als auch andere in ihrem Unternehmen darauf geklickt haben, während 29 % angeben, dass andere im Unternehmen (nicht sie selbst) auf solche Links geklickt haben.

Alarmierend ist, dass ganze 40 % aller Teilnehmenden angaben, ein Passwort für mehrere Zugänge zu verwenden – was den möglichen Schaden von Phishing-Attacken potenziert.

Fast 40 % der Unternehmen erlebten Ransomware-Angriffe – ein Fünftel zahlte Lösegeld

38 % der Teilnehmer berichten, dass ihr Unternehmen 2023 von Malware betroffen war, die Daten oder Hardware verschlüsselte und daraufhin ein Lösegeld für deren Freigabe verlangt wurde. Davon zahlten 8 % der Unternehmen das Lösegeld und konnten ihre Daten zurückerhalten. Allerdings zahlten weitere 11 % das Lösegeld, ohne ihre Daten wiederherstellen zu können. So endeten fast 1/5 der Angriffe mit einer Lösegeldzahlung, wobei über die Hälfte der Zahlungen zwischen 5.000 und 50.000 Euro lag.

36 % der Unternehmen, die kein Lösegeld zahlten, konnten die Ransomware entfernen bzw. ihre Daten selbst entschlüsseln. Weitere 35 % konnten ihre Daten aus einem Backup wiederherstellen. 5 % der Unternehmen akzeptierten einen dauerhaften Datenverlust, da keine Backups vorlagen.

Die bedeutendsten Schwachstellen

Die größten Herausforderungen sehen die Unternehmen dabei in:

- Gedankenlosigkeit von Angestellten (40 %),
- unzureichende Netzwerksicherheit (31 %),
- unzureichende Sicherheit mobiler Geräte (30 %),
- nicht verschlüsselte Daten (30 %),
- Anfälligkeit für Phishing-/Social-Engineering-Methoden (30 %).

Aktuelle Trends zeigen einen deutlichen Anstieg gezielter Ransomware-Angriffe und Phishing-Kampagnen, die durch den Einsatz von künstlicher Intelligenz und maschinellem Lernen immer ausgefeilter werden. Diese Entwicklungen erfordern eine ständige Anpassung und Erweiterung der eingesetzten Sicherheitsstrategien. Da Unternehmen zunehmend auf diese Technologien angewiesen sind, werden Themen wie Cloud-Sicherheit und der Schutz von IoT-Geräten immer wichtiger. Eine risikosensible Strategie bietet Unternehmen die Flexibilität und Reaktionsfähigkeit, sich schnell auf die größten Bedrohungen einzustellen.

Methodik

Um die Daten für diesen Bericht zu erheben, führte Capterra im Zeitraum vom 10. bis 26. November 2023 eine Umfrage unter 1.314 Mitarbeitenden aus Unternehmen jeder Größe in Deutschland durch. Die Teilnehmenden wurden anhand der folgenden Kriterien ausgewählt:

- zwischen 18 und 65 Jahren
- Iin Vollzeit angestellt
- Unternehmen der Befragten nutzen Sicherheitstools.

902 der Befragten waren in die Cybersicherheitsmaßnahmen ihres Unternehmens involviert, sei es

- verantwortlich (233),
- mitwirkend (326) oder
- zumindest darüber informiert (343).

Zusätzlich haben 412 Befragte nur begrenztes Wissen über die Sicherheitsmaßnahmen und beantworteten nur eine eingeschränkte Anzahl an Fragen.

Über Capterra

Capterra ist die erste Adresse, um die richtige Unternehmenssoftware zu finden. Unsere Plattform umfasst mehr als 95.000 Lösungen aus 900 Softwarerubriken und bietet über 1,8 Millionen verifizierte Nutzerbewertungen.

Pressekontakt: Ina Schumann, Ina.Schumann@gartner.com