**Cybersecurity-Trends 2023: ProSoft gibt Ausblick und empfiehlt wichtige Handlungsstrategien**

*IT-Security-Experte sieht steigende Bedrohungsszenarien im KMU- und Industrieumfeld*

Geretsried, im Januar 2023 **– Erhöhte Cybercrime-Aktivitäten, Ransomware- und Distributed Denial of Service-(DDoS)-Angriffe sowie KI-gesteuerte Attacken – das Jahr 2022 verzeichnete eine nie dagewesene Zahl an Cyber-Bedrohungen. Die Ergebnisse präsentierte das Bundesamt für Sicherheit in der Informationstechnik (BSI) jüngst im jährlichen Report. Auch Trusted Advisor ProSoft konnte das erhöhte Aufkommen von Schadsoftware bestätigen und verzeichnete gleichzeitig eine deutlich gestiegene Nachfrage nach Cybersecurity-Lösungen und -Beratung. Dazu Geschäftsführer Robert Korherr: „Wir möchten uns nicht als Krisengewinner bezeichnen, aber sowohl die Corona-Pandemie als auch der geopolitische Konflikt zwischen der Ukraine und Russland und den daraus resultierenden Cyberangriffen auf europäische Verbündete/Nachbarländer sowie Kritische Infrastrukturen hat unser Wachstum positiv beeinflusst.“**

Doch vom erfolgreichen Geschäftsjahr profitierte ProSoft nicht allein, sondern das Unternehmen setzte auf strategische Erweiterung seines Know-hows, was sich gleichermaßen für die Kunden als gewinnbringend auszeichnete. Der Security-Experte investierte in die Rekrutierung neuer Fachkräfte und in Kooperationen mit weiteren Hidden Champions, um branchenübergreifend für Unternehmen sowie staatliche Institutionen passende Security-Lösungen und individuelle Beratung bieten zu können. Denn laut Korherr wurden seitens der Kunden insbesondere Lösungen für die Authentifizierung und das Identitäts-Management (+24 %), das Schwachstellen-Management (+10 %) und zur Cyberabwehr (+54 %) angefragt.

Auch für das Jahr 2023 prognostiziert ProSoft einen Anstieg von Cyberangriffen, empfiehlt nachhaltige Verteidigungsstrategien und warnt vor folgenden kommenden Bedrohungsszenarien:

**Industrieunternehmen im Fokus**

Cyber-Angriffe auf Industrieunternehmen, die zu Betriebsunterbrechun-gen bis hin zu länger anhaltenden Produktionsstillständen führen, werden auch in 2023 deutlich zunehmen. Verantwortlich für die angespannte Situation sind immer wieder neue, intelligente, teils mit KI ausgeführte Angriffsmethoden, aber auch gravierende Software-Schwachstellen in genutzten Betriebs- und Steuerungssystemen. Laut Branchenverband Bitkom sieht jedes zehnte Unternehmen gar seine Existenz durch Cyberangriffe bedroht. Gemäß einer letztjährigen Studie von Trend Micro (<https://resources.trendmicro.com/IoT-survey-report.html>), waren 90 Prozent der deutschen Fertigungs-, Strom-, Öl- und Gasversorgungs-Unternehmen von Mitte 2021 bis Mitte 2022 von massiven Cyberangriffen betroffen. Der finanzielle Schaden belief sich auf durchschnittlich 2,9 Millionen Euro. ProSoft prognostiziert, dass die Schäden auch dieses Jahr in ähnlichen Regionen liegen werden. Es wird angenommen, dass im Durchschnitt 75% der Industriebetriebe im Laufe des Jahres mehrmals Ziel von Cyberkriminellen sein werden. Steht eine Produktion, hat das nicht nur Auswirkungen auf den Kernbetrieb eines Unternehmens, sondern auf ganze Lieferketten und damit indirekt auch auf die Weiterverarbeitung und Lieferfähigkeit anderer Firmen.

**Steigende Schadprogramm-Varianten**

Die Anzahl neuer Schadprogramme und Malware-Varianten hat laut BSI im aktuellen Berichtszeitraum um weitere 116,6 Millionen zugenommen. Durchschnittlich lag die Zahl der täglich neuen [Schadprogramm](https://www.prosoft.de/blog/glossar/backdoor/)-Varianten bei 319.000. Es gibt heute eine Vielzahl an Möglichkeiten, Unternehmen und Organisationen durch Malware Schaden zuzufügen. Die Frage ist heute nicht mehr ob, sondern wann diese betroffen sein werden. Um Cyberkriminellen keine Plattform für gefährlichen Attacken zu bieten, müssen Verteidigungsstrategien ständig überdacht und angepasst werden. Die gute Nachricht: Es gibt Methoden, sich gezielt und dauerhaft gegen die sich ständig verändernden Angriffs-Szenarien zu schützen und IT- sowie OT-Infrastrukturen zuverlässig abzusichern. Durch die Einbettung beispielsweise einer Zero-Trust-Strategie in die eigene Sicherheitsarchitektur erreichen Unternehmen ein Maximum an IT-Sicherheit.

**Mehr Schwachstellen in Soft- und Hardware**

Auch die Schwachstellen in Hard- und Software Produkten werden zunehmen. Meldungen über kritische Sicherheitslücken werden auch in 2023 nahezu täglich kommuniziert werden. Was Unternehmen in dieser Hinsicht optimieren können, ist die Zeitspanne, in der IT-Abteilungen kritische Schwachstellen beheben. Hierfür existieren Lösungen, die einen erweiterten Ansatz verfolgen und über klassisches Patch-Management hinaus gehen, z. B. Benutzer-Authentifizierung an Netzwerk- und Cloud-Ressourcen sowie Endpoint-Security-Analysen. Somit lässt sich nicht nur die durchschnittliche Reaktionszeit beim Patch-Management minimieren, auch notwendige Compliance Sicherheitsstandards lassen sich durch eine integrierte Plattform einhalten, damit Netzwerke und Cloud-Systeme konsequent geschützt bleiben.

**Ransomware – Ausweitung der Erpressungsmethoden**

Nicht neu, aber anhaltend gefährlich sind Ransomware-Angriffe, auch für Privatpersonen. Erpressungsversuche mit erbeuteten Identitäten und Daten wird auch für diesen Personenkreis ein Problem bleiben. Beispielsweise durch Sextortion-Kampagnen, bei denen potenzielle Opfer mit der Veröffentlichung von vermeintlich existierendem, kompromittierendem Material bedroht werden. Ob die Opfer nach wie vor einen bestimmten Betrag in einer Kryptowährung überweisen sollen, um die Veröffentlichung zu verhindern, bleibt angesichts der Kryptokrise allerdings abzuwarten.

**DDoS-Angriffe und Advanced Persistent Threats (APT) nehmen zu**

Neu in den zurückliegenden Monaten ist laut [BSI](https://www.prosoft.de/blog/glossar/bsi/)-Lagebericht 2022 jedoch, dass Cyber-Kriminelle „technisch hoch entwickelte und strategisch intelligente“ DDoS-Angriffe entwickelt haben, die beispielsweise öffentlich verfügbare Störungsmeldungen nutzen (z. B. https://allestörungen.de) und die Angriffsvektoren an die dort gemeldeten Auswirkungen anpassen. Auch die Zahl der [DDoS](https://www.prosoft.de/blog/glossar/ddos/)-Angriffe wird in 2023 weiter zunehmen. Der [BSI](https://www.prosoft.de/blog/glossar/bsi/)-Lagebericht benennt für 2022 ca. 12 operierende [APT](https://www.prosoft.de/blog/glossar/apt/)-Gruppen, die zielgerichtete Cyberangriffe auf Institutionen durchführen, um sich einen dauerhaften Zugriff auf deren Netzwerke zu verschaffen. [Advanced Persistent Threats](https://www.prosoft.de/blog/glossar/advanced-persistent-threats/) ([APT](https://de.wikipedia.org/wiki/Advanced_Persistent_Threat)) dienen hauptsächlich der taktischen und strategischen Informationsgewinnung, aber auch der Spionage und Sabotage von Organisationen und Einrichtungen. Im Fokus der [APT](https://www.prosoft.de/blog/glossar/apt/)-Gruppen stehen dabei in erster Linie wertvolle Schlüsseltechnologien „Made in Germany“, Behörden sowie die diplomatischen Vertretungen einzelner Staaten.

Für diese aktuellen Szenarien bietet ProSoft passende und individuelle Lösungen für sicheren Schutz im Unternehmen an. Weitere Informationen sind bei ProSoft unter der Telefonnummer +49 (0) 8171 405 200 oder per E-Mail an [info@prosoft.de](mailto:info@prosoft.de) erhältlich.

**\_\_\_**

**Über ProSoft**

Gemäß dem Slogan „Manage, Secure, Optimise IT“ steht ProSoft seit der Gründung im Jahr 1989 für effiziente IT-Security & IT-Management-Lösungen. Darüber hinaus arbeitet das Unternehmen mit Premium „Hidden Champions“ und deren Alleinstellungsmerkmalen, um alle Kundenanforderungen exakt zu bedienen und die Lücken der Standardanwendungen zu schließen. ProSoft sorgt mit seinen Managed Services und Support für IT-Sicherheit in der Infrastruktur in Unternehmen – branchenübergreifend. 36 von 40 DAX-Unternehmen und über 5.000 Kunden in der DACH-Region nutzen die Lösungen von ProSoft. Darüber hinaus unterstützt das Unternehmen als Value-Added-Distributor (VAD) Hersteller beim „Go-to-Market“ und der Markteinführung neuer Lösungen im deutschsprachigen Teil Europas. Im Fokus stehen dabei Mehrwerte für Reseller und institutionelle IT-Anwender. Hersteller profitieren von den firmeninternen Marketing- und Vertriebsstrategien und Services wie Webcasts, Events, Partnertrainings, Installations- und Produktsupport.

Mehr Informationen unter [https://www.prosoft.de](https://www.prosoft.de/) sowie unter dem Unternehmens-Blog unter <https://www.prosoft.de/blog/>