**Mit Whitelist-DNS-Filter und Remote-Browser erfolgreich gegen Ransomware**

*IT-Security-Experte ProSoft empfiehlt zwei Verteidigungsstrategien gegen Ransomware-Angriffe auf die Unternehmens-IT*

Geretsried, im Juni 2022 **– Zwölf Prozent aller Cyberangriffe erfolgen inzwischen durch Ransomware\*1. Entsprechende Angriffe haben sich somit in den letzten Jahren vervierfacht. Die finanziellen Schäden, die so ein Angriff verursacht, steigen ebenfalls rasant. IT-Security-Experte, Trusted Advisor und Value Added Distributor ProSoft zeigt mit DNS-Filtering und ReCoBs (Remote Controlled Browser System) zwei wirkungsvolle, aber vom Ansatz her grundsätzlich unterschiedliche Strategien gegen Ransomware-Angriffe. Während ein DNS-Filter gefährliche Websites erkennt und blockiert, bevor Schadcode in das eigene Netzwerk gelangen kann, schirmt ein ReCoBS, also ein ferngesteuerter Web-Browser, das interne Netzwerk vom Internet ab und verhindert präventiv Angriffe, die etwaige Sicherheitslücken in Internetbrowsern ausnutzen. Doch DNS-Filtering ist nicht gleich DNS-Filtering und nur die Summe kombinierter Maßnahmen schützt wirklich zuverlässig.**

Wer Ransomware einsetzt, will sich auf kriminelle Art schnell Geld verschaffen. Dringt die Schadsoftware in die Unternehmens-IT ein, verschlüsselt sie geschäftskritische Daten und macht diese unzugänglich. Die Angreifer fordern im Nachgang für die Entschlüsselung teils beträchtliches Lösegeld. Aus Angst, sensible Firmendaten könnten veröffentlicht oder verkauft werden, zahlen die Opfer oft hohe Lösegeldsummen. „Ob die Angreifer die Daten nach Zahlungseingang wieder freigeben, ist jedes Mal ein Glücksspiel. Betroffen sind hiervon vor allem Unternehmen aus dem Mittelstand sowie mittlere Organisationen – einschließlich Behörden und Unternehmen aus dem Gesundheitssektor\*2“, weiß Robert Korherr, Geschäftsführer der ProSoft GmbH, zu berichten. Gemäß einer Studie zu Ransomware\*3 gaben 70 % der befragten deutschen Unternehmen an, dass die wiederhergestellten Daten teilweise oder ganz beschädigt waren. 80 % der Organisationen, die Lösegeld bezahlt haben, werden ein zweites Mal durch Ransomware attackiert.

**DNS-Filtering ist nicht gleich DNS-Filtering**

Ungewöhnliche DNA-Aktivitäten sind ein untrügliches Anzeichen einer Ransomware-Attacke. DNS-Filter schützen hier dreifach: Drive-by-Downloads aktiver Inhalte von gefährlichen Webseiten werden häufig im Ansatz unterbunden. Das Nachladen von Malware-Komponenten von Command and Control Servern sowie die typische Datenexfiltration vor der eigentlichen Datenverschlüsselung auf Server des Angreifers sind ebenfalls konkrete Anhaltspunkte für eine aktive Ransomware-Phase. Traditionelle, nach dem Blacklisting-Prinzip arbeitende DNS-Filter müssen täglich über 200.000 neue Internet-Domänen erfassen und klassifizieren. Für die Dauer ab der Erkennung bis zur Integration der IP-Adressen von gefährlichen Webseiten in die Blacklist ist die IT anfällig. Whitelisting bietet bei DNS-Filtern dagegen erhebliche Vorteile. Ein Whitelist-DNS-Filter, wie etwa Blue Shield Umbrella, eine Entwicklung des österreichischen Hidden Champions Blue Shield Security, blockiert zunächst alle unbekannten Webseiten und analysiert nur jene, die auch tatsächlich aufgerufen werden. Die eingesetzten Algorithmen und KI-gestützten Technologien des cloudbasierten DNS-Schutzschilds analysieren, erkennen und blockieren Gefahren und Anomalien bei jedem Aufruf in Echtzeit. Erst bei entsprechender Qualifizierung wird die Domain auf die Whitelist gesetzt. Dabei müssen sich die Domains permanent weiter qualifizieren, um auf der Whitelist zu bleiben. Zur Qualifikation nutzt Blue Shield Umbrella Machine Learning aus historischen Daten, eine eigens entwickelte Sandbox und weltweite Kooperationen mit anderen Herstellern und Organisationen.

**Ferngesteuerter Webbrowser für höchste Internetsicherheit**

Ein anderes Tool zur Abwehr von Ransomware-Angriffen stellt das von der Berliner m-privacy GmbH entwickelte ReCoBS TightGate-Pro dar. Die Lösung verfolgt einen anderen Ansatz und schützt vor Ransomware, die versehentlich bereits heruntergeladen wurde. TightGate Pro arbeitet dabei wie folgt: Der Webbrowser wird nicht mehr auf dem Arbeitsplatzrechner ausgeführt. Stattdessen übernimmt der dedizierte, in der demilitarisierten Zone (DMZ) aufgestellte, TightGate-Server die Ausführung des Browsers. Der Arbeitsplatzcomputer erhält lediglich die Bildschirmausgabe des Browsers als Videodatenstrom über ein funktionsspezifisches Protokoll. Aufgrund dieser physischen Trennung bleibt selbst der Aufruf einer kompromittierten Internetseite für das interne Netzwerk folgenlos.

**Summe kombinierter Maßnahmen bietet maximalen Schutz**

Wie jede andere Malware, gelangt Ransomware über die üblichen Kanäle wie Phishing, Spoofing, ungepatchte Sicherheitslücken, Drive-by-Downloads und Schadsoftware in aktiven Internet-Inhalten ins Unternehmensnetzwerk. Technische Maßnahmen wie Antivirensoftware, Log-Management & SIEM, Firewalls, Patch-Management, Endpoint Detection & Response (EDR), Network Detection & Response (NDR) sind einige der Tools, die sich gegen Cyberangriffe bewährt haben. Sicher schützen werden sie jedoch nur, wenn Daten aus unterschiedlichen Quellen korreliert werden. Organisatorische Maßnahmen wie Sicherheitsschulungen und Verhaltensregeln für Mitarbeiter sind ebenfalls eine wirksame Maßnahme, weil eine gewisse Skepsis auch gegen Zero-Day Malware wirkungsvoll ist.

Weitere Informationen gibt ProSoft gerne unter der Telefonnummer +49 (0) 8171 405 200 oder per E-Mail an: info@prosoft.de

**\_\_\_**

\*1 Laut Global Threat Intelligence Report von NTT

\*2 Laut Acronis Cyberthreats Report 2022

\*3 Laut [Cybereason Report 2022](https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf)

**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/>