**ProSoft präsentiert Blue Shield Umbrella: Der weltweit erste KI-basierte Whitelist DNS-Filter**

*Dynamisch lernender DNS-Blocker wehrt Bedrohungen in Echtzeit ab, bevor sie das Netzwerk erreichen*

# Geretsried, im März 2022 – Das Domain Name System (DNS) macht das Internet für Anwender erst richtig nutzbar. DNS wandelt Webseiten-Aufrufe in IP-Adressen um und leitet Anwender-Anfragen an den Zielserver weiter. Aber: DNS ist nicht verschlüsselt und damit eine potenzielle Schwachstelle für jeden Computer und somit auch jedes Unternehmensnetzwerk. Hohes Gefahrenpotenzial besteht beispielsweise durch das Eindringen von Malware und Zero-Day Schadcode, aber auch durch gefakte Websites für Man-in-the-middle-Attacken, Phishing- und Pharming-Angriffe. Bei täglich ca. 200.000 neu registrieren Domänen, wovon 70% als potenziell gefährlich anzusehen sind, bietet klassisches Blacklist Filtering keinen zuverlässigen Schutz mehr. Die Lösung bietet ProSoft mit dem bereits in 2013 entwickelten Whitelist DNS-Filter Blue Shield Umbrella. Dieser erkennt gefährliche Websites und blockiert diese, bevor Schadcode in das eigene Netzwerk gelangen kann. Die neu integrierte Künstliche Intelligenz (KI) und die eigens dafür entwickelte Sandbox-Umgebung machen Blue Shield Umbrella zum weltweit ersten, KI-basierten DNS Whitelist-Filter.

# Blue Shield Umbrella ist eine Entwicklung des österreichischen Hidden Champions Blue Shield Security GmbH. „Im Gegensatz zu herkömmlichen, rein reaktiv arbeitenden Blacklist DNS-Filtern, überprüft Blue Shield Umbrella bei jedem Aufruf einer neuen oder geänderten Webseite diese in Echtzeit auf Gefahren und Malware – vorausschauend und selbstlernend. Hierfür kooperiert der Hersteller mit einigen der weltweit größten NOCs (Network Operations Center) für das Trainieren der künstlichen Intelligenz im Rahmen des Supervised-Learning“, erklärt Robert Korherr, Geschäftsführer der ProSoft GmbH.

# Treffsicher und intelligent

# Die im Hintergrund auf Basis von Algorithmen laufende Prüfung ist dabei so treffsicher, dass beispielsweise auch sogenannte evasive Malware – also Malware, die aufgrund ausgefeilter Tarntechniken von herkömmlichen signaturbasierten Antivirenlösungen nicht identifiziert werden – zuverlässig erkannt wird. Dazu überwacht die Software alle weltweit neu ausgestellten SSL-Zertifikate. Neben Algorithmen mit künstlicher Intelligenz und der Sandbox, werden auch historische Daten wie die Codebewertung inklusive aller versteckten Verzeichnisse, das Verbindungsverhalten sowie IP- und Alternative Nameserver-Reputation kontrolliert. Bei Veränderungen müssen sich Webseiten stets neu qualifizieren.

# Blue Shield Umbrella arbeitet rein dynamisch und ohne Inhaltskategorisierung nach einem „Allow-/Whitelist-Only“ Prinzip, dadurch sind False Positives sehr selten. Durch die Spiegelung der Root-Server mit allen wichtigen Zonen, werden durch die Vorsortierung bereits viele fragwürdige Domains entfernt.

# Zero-Day-Angriffe effizient abgewehrt

# Während herkömmliche DNS-Filter lediglich bekannte „böse“ Domänen sperren, blockiert Blue Shield Umbrella auf Basis der einzigartigen verhaltensbasierten Methodik und des Allow-/Whitelist-Ansatzes auch alle neu entdeckten Sicherheitslücken für die es noch keine Patches gibt (Zero-Days). Die Bewertung einer Domain ist dabei für maximal fünf Minuten gültig, da sich der Status von „Gut“ und „Böse“ jederzeit ändern kann.

# Anwendung des Zero Trust Modells

# Im Zweifelsfall greift das Zero-Trust-Sicherheitskonzept von Blue Shield Umbrella. Dabei wird allen Diensten, Anwendern und Geräten grundsätzlich misstraut und neue oder veränderte Webseiten werden zunächst bis zur Überprüfung blockiert. „Mit Blue Shield Umbrella erfahren Unternehmen eine maximale Reduzierung der Gefahren, die durch die betriebliche Nutzung des Internets ausgehen. Domänen oder Hosts, die plötzlich als malicious oder gehackt gelten, Malware verteilen oder Phishing betreiben, werden schnell erkannt und zuverlässig blockiert. Potenzielle Schäden für Unternehmen werden so von Anfang an vermieden“, resümiert Korherr.

# Flexibel einsetzbar und branchenübergreifend im Einsatz

# Blue Shield Umbrella unterstützt alle gängigen (mobilen) Plattformen (Windows, MacOS, Linux, Android und iOS) auf Basis der modernen Technologie von DNS over HTTPS und ohne VPN. Die Software ist bereits branchenübergreifend erfolgreich im Einsatz, unter anderem bei der Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft ASFINAG, dem Österreichischen Fußball-Bund (ÖFB), dem Batteriehersteller Banner, dem Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) und dem Süßwarenhersteller PEZ.

# Verfügbarkeit

# Blue Shield Umbrella der Blue Shield Security GmbH ist ab sofort für Reseller und Partner bei ProSoft zu beziehen. Weitere Informationen beantwortet ProSoft gerne unter der Telefonnummer +49 (0) 8171 405 200 oder per E-Mail an: info@prosoft.de

**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/>