**ProSoft präsentiert das mobile Kiosksystem MetaDefender K2100 für kritische Infrastrukturen**

*Neue sehr robuste Hardware von OPSWAT erfüllt militärische Standards*

Geretsried, im Mai 2023 **– Viele Industriezweige setzen heute in OT- und ICS-Systemen physikalisch und logisch getrennte Air-Gapped-Infrastrukturen ein. Diese Netzwerke sind nicht nur von IT-Infrastrukturen, sondern aus Gründen der Sicherheit auch von der Internet-Anbindung getrennt. Die Systeme sind damit allerdings auch auf Wechselmedien angewiesen, um Updates zu installieren, Audits durchzuführen und Daten zu übertragen. Wenn diese Wechselmedien jedoch nicht ordnungsgemäß verwaltet werden, können sie potenzielle Schwachstellen und Malware einschleppen, die sich dann im gesamten OT-Netzwerk verbreiten können. Andere Anwendungsbereiche sind aber auch militärische IT-Systeme, Behördennetzwerke oder Systeme zur Steuerung kritischer Infrastrukturen. Trusted Advisor ProSoft empfiehlt für einen effizienten Schutz von KRITIS-Systemen den MetaDefender Mobile Kiosk K2100 von OPSWAT. Dieser stellt eine tragbare, leistungsstarke und extrem robuste mobile Datenschleuse dar, die für den Einsatz unter härtesten Bedingungen konzipiert wurde. Der K2100 entspricht sogar militärischen Standards, verfügt über einen handschuhbedienbaren Bildschirm und ist wasserdicht.**

Die MetaDefender-Kioskserie von OPSWAT wurde entwickelt, um eine potenzielle Sicherheitslücke für kritische Infrastrukturen zu schließen, die durch Air-Gaps geschützt sind. Um diese Systeme zu patchen, sie zu überprüfen oder Daten zwischen ihnen zu verschieben, werden Wechselmedien wie SD-Karten, USB-Sticks und manchmal sogar DVDs von Mitarbeitern oder Dienstleistern verwendet.

**Effizientes Scannen und Bereinigen von Wechseldatenträgern**

Das Risiko besteht dabei in beiden Richtungen: Speziell in der OT oder in physikalisch getrennten Netzwerksegmenten sind es Dienstleister, die CAM- oder industrielle Steuerungssysteme mit Updates unter Zuhilfenahme von Wechseldatenträgern versorgen. Es kann aber auch durchaus vorkommen, dass Konfigurationen über mobile Datenträger „mitgenommen“ werden. Zusätzlich ermöglicht der K2100 ein- und ausgehende Daten auf „Persönlich identifizierbare Informationen“ (PII), Hostnamen und andere sensible Daten zu scannen und die Dateien entsprechend zu bereinigen.

**30 Antivirenschutzanwendungen und Schutz vor Zero-Day-Angriffen**

Der K2100 bietet dazu die Möglichkeit Dateien auf Wechseldatenträgern mit bis zu 34 verschiedenen Antivirenschutzanwendungen parallel zu scannen und Binärdateien und ausführbare Dateien auf Hersteller- und Versionsinformationen zu überprüfen. Dabei wird festgestellt, ob potenzielle Schwachstellen für geschützte Systeme vorliegen. Darüber hinaus nutzt das Kiosksystem eine Technologie zur Entschärfung und Rekonstruktion von Inhalten, um vor Zero-Day-Angriffen zu schützen. „Mit bis zu 34 AV-Engines erreicht der Anwender Erkennungsraten von >99%. Zero-Day Malware kann nur eliminiert werden, wenn alle möglichen Risiken aus Dateien bereinigt bzw. desinfiziert werden“, so Robert Korherr, Geschäftsführer der ProSoft GmbH. Daher wurde die CDR-Technologie (Content Disarm and Reconstruction) im MetaDefender-Kiosksystem so konzipiert, dass sie auch komplexe Dateien von allen Risiken desinfiziert und unter Umständen auch komplett neu erstellt.

**Kritische Infrastrukturen und Militärunternehmen im Fokus**

Zielkunden des neuen Kiosksystems sind die Fertigungs-, Chemie-, Energie- und Ölindustrie. Ferner Ermittlungsbehörden oder das Militär, die digitale Beweise vor Ort sammeln, wie beispielsweise von Kriminellen genutzte Laptops, USB-Sticks und Telefone. Daher präsentiert ProSoft das System auf der diesjährigen **AFCEA** im Saal New York / Genf an **Stand S26**. Die Messe findet vom 10. bis 11. Mai 2023 im World Conference Center in Bonn statt.

Der K2100 ist ab sofort erhältlich. Das Produkt ist entweder als unbefristetes Modell erhältlich – bei dem die Hardware direkt gekauft werden kann, wobei Lizenzgebühren für die AV-Engines und verschiedenste Funktionen anfallen – oder als Abonnement-Modell mit einer jährlichen Leasinggebühr für Hard- und Software. Weitere Informationen sind hier einsehbar: <https://www.prosoft.de/loesungen/cybersecurity/datenschleuse/> oder 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/>

**Über OPSWAT**

OPSWAT ist ein weltweit führender Anbieter von Cybersicherheitslösungen für kritische IT-, OT- und ICS-Infrastrukturen sowie von Deep CDR (Content Disarm and Reconstruction) Sicherheitstechnologien zum Schutz vor Malware und Zero-Day-Angriffen. Um das Risiko einer Kompromittierung zu minimieren, schützen die OPSWAT-Lösungen die kritischen Infrastrukturen von sowohl global operierenden Unternehmen, als auch von Organisationen des öffentlichen und privaten Sektors mit den neuesten Technologien, Prozessen und Hardware-Scans. Mehr als 1.500 Unternehmen weltweit aus den Bereichen Finanzdienstleistungen, Verteidigung, Fertigung, Energie, Luft- und Raumfahrt sowie Logistik & Transport vertrauen auf OPSWAT, um ihre Daten, Dateien und Geräte zu sichern, die Einhaltung von branchen- und behördlichen Richtlinien und Vorschriften zu gewährleisten und ihre Mitarbeiter und Kunden vor cyberbedingten Störungen zu schützen. Für weitere Informationen über OPSWAT besuchen Sie <https://www.opswat.com>

**Medien Kontakt**Kat LewisDirector of Corporate Communications[kat.lewis@opswat.com](mailto:kat.lewis@opswat.com)