

Ihr digitaler
Sicherheitsdienst

DATENSCHLEUSE



Cyberangriffe nehmen exorbitant zu – Einfallstore müssen sofort und wirkungsvoll geschlossen werden!

Seit einigen Jahren erlebt die digitale Welt einen exponentiellen Anstieg durch permanente Angriffe aus dem Internet sowie durch Schadcodeeintrag in die Unternehmen (Malware, Ransomware). Alleine im Jahr In 2020 wurden über **137 Mio.** neue Malware-Varianten registriert (Quelle: BSI sowie Bundeslagebild 2020 „Cybercrime“ des BKA). Täglich werden ca. **375.000 neue Versionen pro Tag** oder **4,3 Versionen pro Sekunde** generiert.

Die Lösung eines einzelnen Endpoint-Schutz-Herstellers (Antivirus-Lösung) kann daher keinen vollständigen Schutz mehr garantieren.

Die Schallmauer, hin zu einer neuen Verfahrensebene der Gewährleistung von IS/IT-Sicherheit im „Cyber“-Raum ist erreicht - wir halten für Sie, mit der **KRITIS-Datenschleuse**, einen wesentlichen Lösungsbaustein bereit.

Ein tatsächlich wirksamer Schutz für das Unternehmen kann neben dem Einsatz von technischen Lösungen darüber hinaus nur erreicht werden, wenn die eigene Prozessorganisation und das etablierte Sicherheitsbewusstsein (Security Awareness) wirksam sind. Im Zusammenhang gehört ein stetiges Aktualisierungs- und Änderungsmanagement zur Abwehr von Malware zu den wichtigsten Säulen gegen Cyberangriffe aller Art, um nicht von einer Ransomware infiziert zu werden, wie dies unlängst bei sehr bekannten Unternehmen wie beispielsweise Acer, Maersk, Pilz und Tegut zu verzeichnen war.

Unsere schnell einsetzbaren und effektiven Startup-Bundles der KRITIS-Datenschleuse von OPSWAT, für eine offensive Sicherheitskonzeption



Zentrales Dateien-Desinfekt-Terminal

- für den Einsatz am zentralen Standort oder Sicherheitsbereichen
- für Mitarbeiter, Besucher, Geschäftspartner und Dienstleister

Mobile Datei-Desinfekt-Station via Notebook

- für den flexiblen Einsatz an jedem Betriebsstandort
- für Mitarbeiter und externe Mitarbeiter (Wartungspersonal)

Arbeitsweise:

- die Datenschleuse überprüft alle Medien auf Malware, Schwachstellen und sensible Daten via branchenführenden Multi-Scan (bis zu 35 der weltbesten Antiviren-Scan-Engines möglich)
- löscht kritische Dateien oder -fragmente, wie Skripte und Makros
- speichert die bereinigten Daten manipulationssicher ab
- regelmäßige Überprüfung digitaler Signaturen und Zugriffsverweigerung von Medien, die nicht gescannt und geprüft wurden



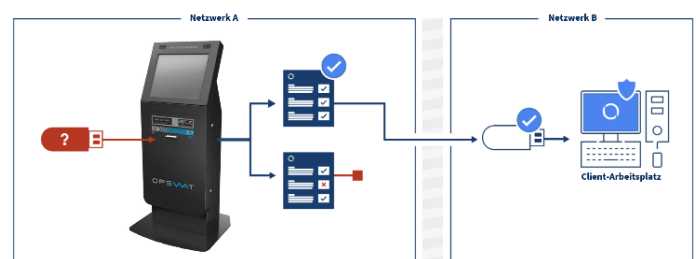
Anwendungsfälle:

- Kopieren von externen USB- und Wechseldatenträgern auf ausschließlich vom Auftraggeber bereitgestellte sowie zugelassene Medien, ohne externen Kontakt und Zugriff
- sichere Übergabe weiterer Datenbestände wie Projektunterlagen, etc.
- Einlagerung von externen Dateien zur Analyse in Sandbox
- Secure Internal Transit in Hochsicherheitsbereiche sowie in unterschiedliche Netzhoheiten

Vorteile & Effekte:

- sehr schnelle Einführung der Lösung, ohne Komplexintegration („ready2run“ innerhalb kurzer Zeit)
- Umgangs- und Bewusstseins-Schärfung bei Mitarbeitern und externen Partner für IT-/Informationssicherheit
- Reputationssteigerung und -sicherstellung bei Kunden und Geschäftspartnern
- Einhaltung von Compliance-Anforderungen von regulierten Branchen/Sektoren
- alle Transaktionen werden protokolliert und nachweisbar aufgezeichnet

Datenschleuse zu Client



CONTROLNET GmbH
Bauhausstraße 7c, 99423 Weimar
Central: +49 (0) 3643 9085 051
Fax: +49 (0) 3643 9085 052

CRITICAL INFRASTRUCTURE PROTECTION
ENERGY | KRITIS | UTILITY | INDUSTRY
www.controlnet.de info@controlnet.de