



S-Web

Sicherer Internetzugang zur Abwehr von digitalen Gefahren

Themenbereich: Sicherheit

Messe-Stand: SI04

Fragen beantwortet
Ihnen Ihre zuständige
Kundenberatung

Ein sicherer und performanter Internetzugang wird immer wichtiger

Über das Produkt »S-Web« wird den Instituten ein sicherer Internetzugang für die Mitarbeiter und sonstige Arbeitsplätze zur Verfügung gestellt. Dabei werden die zwei Lizenzarten »S-Web: Comfort« und »S-Web: Institut Basispreis Virenschanner« (hierfür benötigt das Institut einen eigenen Proxy) unterschieden. Für unverschlüsselte Verbindungen haben beide Lizenzarten einen zentralen Virenschutz. Zusätzlich wird in »S-Web« ein zentraler Scanner (APT) eingesetzt, um verdächtige Verbindungen in einem Sandboxing-Verfahren zu überprüfen. Wird ein Virus gefunden, wird dieser blockiert und der aufrufende Mitarbeiter darüber informiert. Erweisen sich verdächtige Verbindungen bei der Überprüfung als schädlich, werden die erkannten Ziele blockiert. Ergänzend kommen S-CERT-Sperrlisten zum Einsatz. Dabei werden vom SIZ ständig aktualisierte Listen mit Phishing-Servern, maliziösen Web-Seiten und Trojaner-Steuerungs-Servern bereitgestellt und der Zugriff darauf automatisch gesperrt.

Die Leistung »S-Web: Comfort« kann noch mehr

Die Administration der einzelnen Nutzer erfolgt durch das Institut über die OSPlus-konforme Client-/Server-Infrastruktur mit Hilfe von Benutzergruppen im Windows Active Directory. Das Institut kann dabei jedem Mitarbeiter eines von sieben bereitgestellten Profilen des Web-Filters zuordnen. Nachstehend sind die Schutzfunktionen beschrieben:

Bedarfsgerechter Zugriff mittels Web-Filter und Profilen

Der Web-Filter, der von einem externen Dienstleister gepflegt wird, ist eine leistungsstarke Lösung für die Filterung von Internetadressen auf Basis von Profilen. Damit können die nutzenden Institute ihre Benutzer und Netzwerke vor Spyware, Phishing, Peer-to-Peer-Datenaustausch (P2P), Viren und anderen Bedrohungen schützen.

Überprüfung verschlüsselter Verbindungen

Bei der SSL-Interception wird die verschlüsselte Verbindung auf zentralen Systemen der

Bitte umdrehen >>



Seite 02

FI (Blackbox-System) terminiert, der Datenstrom auf Virenbefall geprüft und wiederum verschlüsselt dem Nutzer bereitgestellt. Ausgenommen hiervon sind Verbindungen, die aufgrund von Bestimmungen zum Datenschutz oder aus technischen Gründen nicht terminiert werden dürfen.

Download-Schutz mittels Dateityp-Filter

In den meisten Profilen wird der Download von ausführbaren oder interpretierbaren Dateien bestimmter festgelegter Dateitypen unterbunden.

Zentrale Zertifikate als optionale Leistung

Die Finanz Informatik ermöglicht über zentral in der FI vorgehaltene Zertifikate einen abgesicherten Zugang zu zertifikatsbasierten Anwendungen verschiedener Produktanbieter. Unter anderem hosten wir Zertifikate von DWP-Bank, DekaBank, Payment-IT und Sparkassenversicherung (BaV).

Reporting als optionale Leistung

Die Auswertung der Internetnutzung wird immer wichtiger – sei es, um einen Überblick über die Nutzung zu erhalten, regulatorischen Anforderungen zu genügen oder im Verdachtsfall zur Beweissicherung. Dazu halten wir die Daten 70 Tage vor und bieten verschiedene Auswertungen an:

- Top-100-URL-Auswertung (als regelmäßige monatliche Leistung)
- statische Monatsauswertung (einmalig): Bereitstellung von Tageslogs

Fragen beantwortet
Ihnen Ihre zuständige
Kundenberatung.