SOPHOS

Checkliste: Maßnahmen, Technologien und Tools für wirksamen Webschutz

Zu einer wirksamen Webschutz-Strategie gehören Maßnahmen zur Verkleinerung der Angriffsfläche sowie dafür geeignete Technologien und Tools. Eine gute Sicherheitslösung muss außerdem Angriffe auf allen Ebenen zuverlässig stoppen.

Prüfen Sie mit unserer Checkliste, ob Sie alle erforderlichen Maßnahmen, Technologien und Tools nutzen, um effektiven Schutz für Sie und Ihre Mitarbeiter zu gewährleisten.

Wichtigste Maßnahme: Klare Richtlinien

☐ Richtlinie für sicheres Surfen im Netz

Sperren Sie unerwünschte und unangemessene Website-Kategorien, um Ihre Angriffsfläche zu verkleinern. Ihre Richtlinie sollte mindestens die folgenden Kategorien ausschließen:

- Pornografie
- Anonymisierende Proxyserver
- Kriminelle Aktivitäten, Hacking
- Glücksspiele
- Drogen, Alkohol und Tabak
- Aufrufe zu Rassismus und Diskriminierung
- Phishing, Betrug, Spam, Spyware
- Geschmacklose, anstößige Inhalte
- Gewalt und Waffen

Unter Umständen ist es sinnvoll, weitere Kategorien zu sperren, damit Mitarbeiter weniger Zeit mit Surfen verbringen und die Bandbreite nicht unnötig beansprucht wird.

☐ Richtlinie für sichere Passwörter

Führen Sie Richtlinien zur Erstellung sicherer Passwörter ein. Diese sollten sich an folgenden Regeln orientieren:

- Erstellen Sie ein langes Passwort
- Wählen Sie ein Passwort, das Ziffern, Symbole sowie Klein- und Großbuchstaben enthält
- Verwenden Sie keine Begriffe aus dem Wörterbuch
- Verwenden Sie keine persönlichen Informationen wie Namen oder Geburtstage
- Ändern Sie Ihr Passwort regelmäßig
- Notieren Sie sich keine Passwörter

☐ Richtlinie zur Kontrolle von Anwendungen

Regeln Sie mit einer Richtlinie, welche Webbrowser, Anwendungen und Plug-ins in Ihrem Unternehmen genutzt werden dürfen. Beschränken Sie sich dabei auf eine überschaubare Auswahl.

- Browser: Beschränken Sie sich auf einen Standard-Browser, der
- Googles Safer Browsing API unterstützt (z. B. Google
- Chrome, Mozilla Firefox oder Apple Safari).
- Java: Erlauben Sie die Nutzung von Java nur ausgewählten Personen, die Java wirklich benötigen; ist die Software nicht zwingend erforderlich, entfernen oder deaktivieren Sie diese
- PDF-Reader: Nutzen Sie nur einen einzigen PDF-Reader und patchen Sie diesen regelmäßig.
- Mediaplayer: Vermeiden Sie unnötige Mediaplayer-Add-ons und Codec-Pakete. Wenn möglich, nutzen Sie den Player Ihres Betriebssystems und installieren Sie regelmäßig aktuelle Patches.
- Plug-ins, Add-ons und Toolbars: Vermeiden Sie unnötige Browser-Plug-ins und Toolbars.

☐ Richtlinie zur Patchverwaltung

Aktivieren Sie für die folgenden Anwendungen eine automatische Aktualisierung. Achten Sie darauf, dass Benutzer Updates und Patches installieren, sobald diese verfügbar sind.

- Webbrowser
- Java
- PDF-Reader
- Flash-Player

Technologien und Tools

☐ URL-Filterung
Zur Durchsetzung Ihrer Richtlinie für sicheres Internet-Surfen benötigen Sie einen wirksamen URL-Filter. Der URL-Filter sollte Sie nicht mit Hunderten von Kategorien überhäufen. Ausnahmen zu den Richtlinien sollten sich einfach einstellen lassen. Er sollte es Benutzern ermöglichen, einfach Anfragen zu Ausnahmen zu übermitteln, die von Ihrer IT-Abteilung mit wenigen Klicks bearbeitet werden können.

☐ Filterung schädlicher Websites
Um sich vor schädlichen Websites zu schützen, benötigen Sie eine wirksame Reputationsfilterung. Eine gute Lösung sollte eine Echtzeit-Aktualisierung bieten. Der Anbieter der Lösung sollte zudem über ein globales Team von Analysten verfügen, das konstant prüft, ob Websites neu infiziert wurden.

☐ Blockierung anonymisierender Proxys
Halten Sie Benutzer in Schach, die Ihre Richtlinien umgehen wollen – mit Technologien, die anonymisierende Proxyserver zum Umgehen der URL-Filterung sperren. Suchen Sie nach einer Lösung, die Anonymizer sowohl anhand von Kategorien sperren als auch in Echtzeit erkennen kann, damit sich neue, verschleierte oder private Proxys so schnell wie möglich sperren lassen.

☐ Spam-Filterung
Ihre Anti-Spam-Lösung sollte die neuesten Technologien nutzen, um Phishing-E-Mails und E-Mails mit sonstigen Schadlinks zu sperren – denn diese sind einer der häufigsten Eintrittspunkte für moderne Webangriffe.

☐ Hochentwickelte Scans auf Internet-Malware
Ihr gesamter Internetverkehr sollte mit modernsten Technologien zur Abwehr von Malware gescannt werden. Eine gute Lösung scannt den gesamten Internetverkehr (nicht nur gefährliche Websites), ohne dabei die Latenz oder die Performance zu beeinträchtigen. Ihre Lösung sollte außerdem moderne Verfahren wie JavaScript-Emulation anwenden, mit denen sich selbst verschleierte und polymorphe Bedrohungen erkennen lassen.

☐ Netzwerk-Sandbox
Ziehen Sie die Implementierung einer Netzwerk-Sandbox in Betracht, die Ihren Web- und E-Mail-Schutz erhöht, indem sie auch Malware abfängt, der es gelingt, herkömmliche Abwehrmaßnahmen zu überlisten.

☐ HTTPS-Scanning
Schließen Sie eine große Sicherheitslücke: mit einer Webschutz-Lösung, die selbst verschlüsselten Datenverkehr scannt. Die Lösung sollte die Performance nicht beeinträchtigen und die Privatsphäre der Benutzer wahren, wenn diese Online-Banking-Seiten besuchen oder andere Finanz-Transaktionen online durchführen.

☐ Call-Home-Erkennung
Außerdem sollte die Lösung bei einer Infektion die infizierten Computer in Ihrem Netzwerk daran erkennen können, dass diese Anfragen an bekannte Malware-Command-and-Control-URLs senden.

☐ Schutz außerhalb des Büros
Schützen Sie Benutzer auch außerhalb des Unternehmensnetzwerks: mit einer Lösung, die Endpoint-Webschutz oder cloudbasierte Filterung bietet. Der Endpoint-Webschutz kann in Ihren Desktop-Virenschutz integriert werden. So haben Sie weniger Client-Software zu verwalten und verfügen über Webschutz ohne Backhauling oder Umleitungen für Cloud-Scans. Bei einer guten Lösung lässt sich der Schutz für Benutzer außerhalb des Büros über die gleiche Konsole zu verwalten wie der für Benutzer innerhalb Ihres Netzwerks.

☐ Echtzeit-Updates
Stellen Sie sicher, dass Ihr System Live-Updates ohne Verzögerung an Sie überträgt. Stündliche oder einmal tägliche Updates der Bedrohungsdaten sind heutzutage nicht mehr ausreichend.

☐ Application Control
Unterbinden Sie mit Richtlinien für Webanwendungen die Installation und Ausführung unerwünschter Anwendungen an den Endpoints. Eine Anwendungsfilterung am Netzwerk-Gateway ist zwar hilfreich, bietet aber keinen Ersatz für eine Anwendungskontrolle an den Endpoints.

☐ Patch-Analyse
Vereinfachen Sie die Durchsetzung Ihrer Patch-Strategie: mit einer Lösung, die wichtige Sicherheitspatches für Ihre Webclient-Software erkennt und priorisiert.

☐ Antivirus mit HIPS
Wählen Sie ein Endpoint-Desktop-Antivirusprodukt mit integriertem HIPS (Host Intrusion Prevention System) und vorkonfigurierten HIPS-Regeln. So müssen Sie nicht erst selbst die optimalen Einstellungen für effektiven Schutz ermitteln.

Optimaler Schutz: Sophos Web Protection

Bei Sophos nutzen wir modernste Technologien, mit denen Sie auch vor neuesten Bedrohungen optimal geschützt sind. Zudem verfügen wir mit den SophosLabs über ein globales Team aus Analysten, die rund um die Uhr für Sie im Einsatz sind. Sie beobachten das Internet konstant, um aktuelle Bedrohungen direkt zu entdecken, und aktualisieren Ihre Systeme sofort, sobald neue Bedrohungen auftauchen.

Besonders wichtig ist uns die Benutzerfreundlichkeit: Eine gute Sicherheitslösung sollte nicht nur wirksam schützen, sondern sich auch einfach bereitstellen und verwalten lassen. Sicherheit leicht gemacht

Sie möchten gerne mehr Informationen zu diesem Thema?
Lesen Sie unser kostenloses Whitepaper „Die fünf Phasen eines Web-Malware-Angriffs“
Zum Download

Sophos Secure Web Gateway
Jetzt testen auf www.sophos.de

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

21.06.2016 WP-DE (GH)

SOPHOS