SOPHOS

Technologien, Tools und Taktiken für wirksamen Webschutz: Checkliste

Um wirksamen Webschutz zu erhalten, benötigen Sie drei essenzielle Dinge: Leistungsstarke Technologien, geeignete Tools sowie die richtigen Taktiken zum Stoppen von Angriffen auf allen Ebenen.

Die folgende Checkliste zeigt Ihnen, welche bewährten Taktiken Sie anwenden sollten und welche Technologien und Tools unerlässlich sind, um sich und Ihre Mitarbeiter optimal zu schützen.

Taktiken: Führen Sie klare Richtlinien ein

☐ Richtlinie für sicheres Surfen im Netz

Sperren Sie unerwünschte und unangemessene Webseiten-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 eine Richtlinie 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: Nutzen Sie nur einen einzigen Browser, der Googles Safer Browsing API unterstützt (z. B. Chrome, Firefox oder 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 überflüssige 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: Wehren Sie Bedrohungen effektiv ab

☐ **URL-Filterung**
Der URL-Filter sollte Sie nicht mit Hunderten von Kategorien überhäufen. Ausnahmen zu den Richtlinien sollten sich einfach einstellen lassen. Der Filter sollte es Benutzern ermöglichen, einfach Anfragen zu Ausnahmen zu übermitteln, die von Ihrer IT-Abteilung mit wenigen Klicks bearbeitet werden können.

☐ **Filterung schädlicher Webseiten**
Um sich vor schädlichen Webseiten zu schützen, benötigen Sie eine wirksame Reputationsfilterung. Eine gute Lösung bietet eine Echtzeit-Aktualisierung. Der Anbieter der Lösung sollte zudem über ein globales Team von Analysten verfügen, das konstant prüft, ob Webseiten 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**
Verificare che la soluzione antispam utilizzata sia impostata su tecnologie aggiornate per il blocco dei messaggi di posta indesiderati, inadeguati, contenenti link di phishing o altro malware — difendendo così uno dei principali punti di accesso dei moderni attacchi Web.

☐ **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 Webseiten), 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.

☐ **HTTPS-Scans**
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**
Eine gute Löosung erkennt infizierte Computer in Ihrem Netzwerk daran, 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. 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**
Ihr System sollte Live-Updates sofort bereitstellen. Stündliche oder tägliche Updates gegen Bedrohungen sind heute 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 bevorzugt einspielt.

☐ **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 Benutzerfreundlichkeit: Eine gute Sicherheitslösung sollte nicht nur wirksam schützen, sondern sich auch einfach bereitstellen und verwalten lassen. Mit Sophos Web Protection erhalten Sie genau das – umfassende Sicherheit, die einfach funktioniert.

Sie möchten zu diesem Thema mehr erfahren?
Lesen Sie unser kostenloses White Paper "Die fünf Phasen eines Web-Malware-Angriffs".
Zum Download

Kostenlose Testversionen auf sophos.de

Sophos Secure Web Gateway
Sophos Enduser Web Suite

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

NP 10/13 NSG na

SOPHOS