SOPHOS

This Is Next GEN WEB SECURITY

Checklist of Technology, Tools and Tactics for Effective Web Protection

An effective web protection strategy requires policies to reduce the surface area of attack, appropriate tools and technology to enforce those policies, and protection to block attacks at every layer.

Establish the following best-practice policies and educate your user population about why they are important for the security of your organization.

Web Protection Policy Checklist

☐ Safe surfing policy

Block unwanted and inappropriate site categories to reduce the threat surface area. As a minimum your policy should exclude the following categories:

- Adult, sexually explicit, nudity
- Anonymizer proxies
- Criminal activity, hacking
- Gambling
- Illegal drugs, alcohol and tobacco
- Intolerance and hate
- Phishing, fraud, spam, spyware
- Tasteless and offensive
- Violence and weapons

You may also wish to control other categories in the interest of productivity or bandwidth.

☐ Strong password policy

You should enforce policies for creating strong passwords, following these guidelines:

- Use long passwords
- Include numbers, symbols, and upper- and lowercase characters
- Don't use common dictionary terms
- Don't use personal information such as names or birthdays
- Change passwords frequently
- Don't write passwords down

☐ Application control policy

Limit the number of Internet browsers, applications and plugins in your organization to a standardized set and enforce their use as policy.

- Browser: Stick with a single mainstream browser that
- supports Google's Safer Browsing API such as Google
- Chrome, Firefox, or Apple Safari
- Java: Unless you require Java for business-related web applications, disable or remove it, or limit it to only those who require it
- PDF reader: Use a single mainstream PDF reader and keep it patched
- Media player: Avoid unnecessary media player addons and codec packs. If possible, stick with what your operating system provides and keep your OS patched
- Plugins, add-ons and toolbars: Avoid unnecessary browser plugins and toolbars

☐ Patch management policy

Make sure the following applications have auto-updates activated where possible and that users are actively applying updates or patches as they become available.

- Web browser
- Java
- PDF reader
- Flash player

To enforce your policies and provide protection from the latest web attacks, you need the following technology and tools.

Web Protection Technology and Tool Checklist

□ URL filtering

To enforce your safe surfing policy, you need an effective URL filter. Look for a solution that doesn't overwhelm you with hundreds of categories, with simple policy exceptions. Your solution should enable users to easily submit an exception request and your IT team to handle it with just a few clicks.

□ Malicious site filtering

For protection from malicious sites, ensure you have effective reputation filtering. Look for a solution that's updated in real time by a vendor with a global threat analysis operation that tracks newly infected sites continuously.

□ Anonymizing proxy blocking

Keep rogue users in check with technology that can block the abuse of anonymizing proxies to bypass URL filtering. Look for a solution that includes both anonymizer category blocking and dynamic anonymizer detection in real time to block new, obscure or home-based proxies.

□ Spam filtering

Be sure your anti-spam solution is using the latest technology to block unwanted and inappropriate emails with phishing or other malicious links—one of the major entry points for a modern web attack.

□ Advanced web malware scanning

All your web traffic should be scanned by the latest advanced web malware technology. Look for a solution that scans all web traffic (not just dangerous sites) and does so without impacting latency or performance. Ensure the solution you have uses the latest technology like JavaScript emulation to detect obfuscated or polymorphic threats.

□ Network sandbox

Consider extending your web and email protection by deploying a network sandbox to capture unique malware that can evade traditional defenses

□ HTTPS scanning

Cover a major blind spot in your web protection with a web security solution that scans encrypted traffic. Ensure the solution doesn't impact performance and that you can preserve the privacy of users visting online banking or financial sites.

□ Call-home detection

In the event of an infection, ensure your solution can identify infected computers on the network by their requests for known malware command-and-control URLs.

□ Offsite protection

Protect users off the corporate network by using a solution that offers endpoint web protection or cloud based filtering. Endpoint web protection can be integrated with your desktop antivirus, reducing the client software you need to manage, and offering web protection without backhauling or redirecting for cloud scanning. Look for a solution that allows you to manage your offsite users with the same console as your users inside the network.

□ Real-time updates

Ensure your system provides live updates with no delay. Hourly or daily updates to threats are no long adequate.

□ Application control

Enforce your web application policy with the right tools to block unwanted applications from installing or running at the endpoint. Although network gateway application-level filtering can be helpful for productivity and bandwidth control, it's important to enforce application control at the endpoint.

□ Patch assessment

Make enforcement of your patch strategy easier with a solution that can identify and prioritize the most important security patches for your selected web client software.

□ Antivirus with HIPS

Choose an endpoint desktop antivirus product with host intrusion prevention system (HIPS) technology built in. Look for a solution that embeds best-practice HIPS rules instead of forcing you to figure out the most effective threat protection settings on your own.

Sophos Web Protection

In addition to this important list of technology, make sure it's backed by an IT security vendor that's committed to best protection. Look for a vendor with a global threat analysis operation that is constantly monitoring the web for the latest threats and providing you instant updates to emerging threats.

Also look for a solution that not only provides effective protection, but is simple to deploy and manage. Simple security is better security.

Interested in learning more?
Get our free guide to the Five Stages of a Web Malware Attack
Download now

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK

2016-06-21 WP-NA (GH)

SOPHOS