SWITCH DNS Firewall

Factsheet

DNSFW DE 3.2017

The SWITCH DNS Firewall service is intended to complement existing web security services by significantly reducing operating risks, the focus being on global cyberattacks. The aim is to prevent infections and identify systems that are already infected, all with a minimum of effort. This creates scope for significant cost savings in ICT support.

SWITCH DNS Firewall protects all your devices that use the DNS service

Added value through using SWITCH DNS Firewall

Domain Name Service Response Policy Zones (DNS RPZ) make it possible to overwrite specific DNS information in order to generate alternative responses to DNS queries. This provides a useful mean to prevent users from calling up malicious domains and reroute them to a secure site.

Prevention
Blocking access to infected sites can counteract an internal infection.

Detection
Computers that are already infected can be detected by SWITCH. Customers are informed rapidly about suspicious and infected computers via security reports.

Awareness
A customizable landing page makes it possible to raise awareness among users accessing a website.

The biggest advantage of DNS RPZ technology is that all devices (including mobile devices and servers) can be effectively protected against malicious external systems even before a connection is established.

Your benefits: SWITCH threat intelligence

Thanks to a unique mix of up-to-date and relevant data compiled by SWITCH-CERT from its national and international work, you receive an unparalleled, Swiss-focused threat list for your users.

This draws on the broad-based security know-how SWITCH-CERT has built up over many years, specifically in the following areas:

- → Analysis of current malware
- → Analysis of malicious domains through operation of the registry for the .ch and .li TLDs.
- → Analysis and qualification of national and international data feeds

«CERN is using SWITCH's DNS Firewall since Q4 2015 for pro-actively preventing our user community accessing malicious domains and phishing web-sites. Using the SWITCH DNS Firewall, unfortunate users are redirected to an internal webpage informing them about the risks of browsing the WWW. So far, we have made great experience with it, also thanks to the quick response of SWITCH to our queries and input, and observed no false positives nor mayor issues.»

– Stefan Lüders, CERN

SWITCH

SWITCH DNS Firewall

DNSFW.DE 3.2017

Service levels

SWITCH DNS Firewall is available in the following variants:

Pure RPZ zone transfer: The malicious domain names collected by SWITCH-CERT are bundled together and sent to the organisation's DNS system.

Pure RPZ zone transfer with notification of potentially infected computers: Reports containing details of infected computers are e-mailed to the organisation's security contacts. These reports are based on DNS Firewall log data supplied by the organisation.

Optional extra: Requests for malicious domains can be rerouted to a landing page that the organisation can customize itself and that informs end-users about the blocked access.

Technical requirements

Integrating the DNS Firewall service is simple thanks to fast activation of DNS RPZ on the DNS resolvers. This requires DNS server software that supports RPZ or a DNS appliance on which DNS RPZ can be activated.

SWITCH has a broad knowledge to advise you on connection and integration.

DNS server software

- BIND
- PowerDNS Recursor
- Knot Resolver

DNS appliances

- Infoblox
- BlueCat
- EfficientIP
- Nokia VitalQIP

«We have been using DNS Firewall at HSR since the start of July 2015. We use the Response Policy Zones managed by SWITCH, with hits analysed by SWITCH as well. This has led to a significant improvement in malware prevention and detection with a relatively small amount of effort. Even though we are logging quite a lot of hits, the level of acceptance among our users is very high. Generally speaking, DNS Firewall has become an efficient cornerstone of IT security at HSR.»

– Roman Rüegg, Hochschule für Technik Rapperswil

Contact

SWITCH
Security / University & Registry
www.switch.ch/security
cert@switch.ch

SWITCH