How DNS Filtering and Website Categorization Lists Can Empower In-House Cybersecurity Teams

Posted on October 28, 2019

The IT security climate these days is pretty unpredictable. A study by the University of Maryland states that a security incident occurs every 39 seconds. Companies around the world are, in fact, increasingly suffering from Web-based attacks, not to mention the fact that the average cost of a data breach has skyrocketed.

The good news is that there is a wide range of measures that in-house cybersecurity professionals can employ against threats. One effective solution is Domain Name System (DNS) filtering.

Depending on how it is implemented, DNS filtering can provide advanced network setting controls to enhance online safety. It can protect organizations from threats like botnet, phishing, and other malware-instigated attacks. The great thing about it is that a website categorization database can supplement it. Such a database is thus an excellent resource for managed security service providers (MSSPs) and the like.

DNS Filtering Basics

In essence, DNS filtering is a method of blocking or restricting access to specific domains or websites on the Internet. By doing so, this approach provides organizations with the protection they need to ensure a safer working environment.

DNS filtering can effectively allow companies to employ advanced network security configurations at the domain level. For instance, users arriving at a malicious website are instead redirected to a secure page by a DNS filtering solution. This will, of course, depend on how the solution is configured.

DNS filters can also be employed to block access to web pages under specific categories. Pages with content related to pornography, gambling, illegal file sharing, and the like can be tagged as unsafe. Because classification needs to happen in real time, a DNS filter needs to be a low-latency solution. It should not delay access to websites, particularly those that are considered safe.

By default, most DNS filtering solutions offer a certain level of protection against malware. There are also more advanced solutions that can detect and block access to phishing websites and other malicious pages.

The Benefits of DNS Filtering

A DNS filtering solution offers several key advantages. One of the most important is the ability to block access to compromised websites and other malicious domains. These pages include “objectionable” sites such as those that host content related to violence, terrorism, and others.

DNS filtering solutions are also scalable, fast, and lightweight. Enterprise-level offerings come with even greater flexibility for customization. With these, security teams can easily input their desired configurations.

Proactively blocking potentially malicious websites may, however, be the main advantage of using a DNS filtering solution. This practice is especially crucial since human error has been identified as the most common cause of cyber incidents. When complemented by a **website categorization list**, for instance, internal security teams can improve defenses against online threats.

Company owners also get the added benefit of preventing employees from accessing prohibited materials such as those that decrease productivity or are offensive to others during work hours.

DNS Filtering Limitations

Despite being a powerful technology, DNS filtering does come with its limitations. Since it is tied to DNS, its filtering and protective approaches are restricted to DNS boundaries. It can only act onthe domain and subdomain levels. It does not offer users any visibility at the page level. As such, teams won't tag a domain as dangerous if only one page on it has a malicious payload.

Blocking harmful content requires website categorization. DNS filtering solutions on their own don't analyze websites for redirection or blocking. They depend on an external source of data for that. If you plan to employ a DNS filtering solution, you should first understand the security and granularity that it offers.

It can, however, go a long way in improving an in-house security team's capabilities. It does so by providing them with the essential infrastructure to protect both the network and its users. However, DNS filtering requires organizations to have a robust strategy and help from trusted third parties (APIs, feeds, etc.).

By itself, DNS filtering lets companies enforce comprehensive and forward-thinking Internet usage policies. These same policies let them block access to potentially harmful websites and threats. Any company is always a potential target, but it can significantly reduce the chances of being compromised.

WhoisXML API offers a machine learning (ML)-powered website categorization API and database that complements DNS filtering solutions. We parse more than 150 million websites and crawl millions more on a daily basis.

All of our data sets are well-parsed and normalized for consistency. Users can download both parsed and raw data in the form of a CSV file or a database dump. Our consolidated and coherent data makes integration with existing systems and processes easy. If you'd like to learn more about what we have to offer, contact us today.