The cybersecurity tools that every business should know

Enterprises have become the main target for most cybercrime as well as violations on the internet due to the nature of data and information of extremely high economic value that they are handling as well as hosting.

With the general situation of cybersecurity being increasingly complicated nowadays, security experts are still going out every hour across technology forums that the cyberattacks will increasingly spread. Broad and continues to pose serious threats to all technology users, from individual users, businesses to government agencies.

In particular, especially businesses - has become the main target for most cybercrime as well as internet violations due to the nature of the data and information of extremely high economic value that they are dealing with. storage as well as storage.

In 2018, the world has witnessed a series of serious data violations targeting many large businesses, leading to the loss of personal and financial records of millions of customers. up to billions of dollars. Specifically, the number of data breaches confirmed in 2018 has reached 12,449 cases, an increase of 424% compared to 2017. This is an alarming situation that more than anyone else will have to know for themselves. How to protect yourself before asking for involvement from relevant agencies.

1. McAfee expert explained how deepfake and AI are drilling through the cyber security wall

Becoming a victim of cyber attacks has never been a pleasant 'experience' for even large businesses because of the huge financial losses they cause. According to calculations, the average processing cost for each enterprise-level attack has increased to $ 1.1 million - a figure that is not small at all. Such losses can completely bring small and medium enterprises to the path of bankruptcy.

According to statistics, up to 60% of small businesses are forced to close within 6 months after the 'security disaster' when unable to remedy and restore business to the status quo. But apart from economic losses, the main factor contributing to 'defeating' companies after an information security incident is the loss of credibility and trust of customers and partners.

After a series of issues mentioned above, it is probably not necessary to say more about the urgency in improving, protecting the security infrastructure and enterprise-level information networks to combat unpredictable developments from the network attack.

Fortunately, the field of global network security is constantly changing, improving to keep up with the development of threats on the internet space. Here are 5 tools that we think all businesses should consider adding to their 'strategic defense weapons' repository to enhance their defenses and minimize any possible risks. .

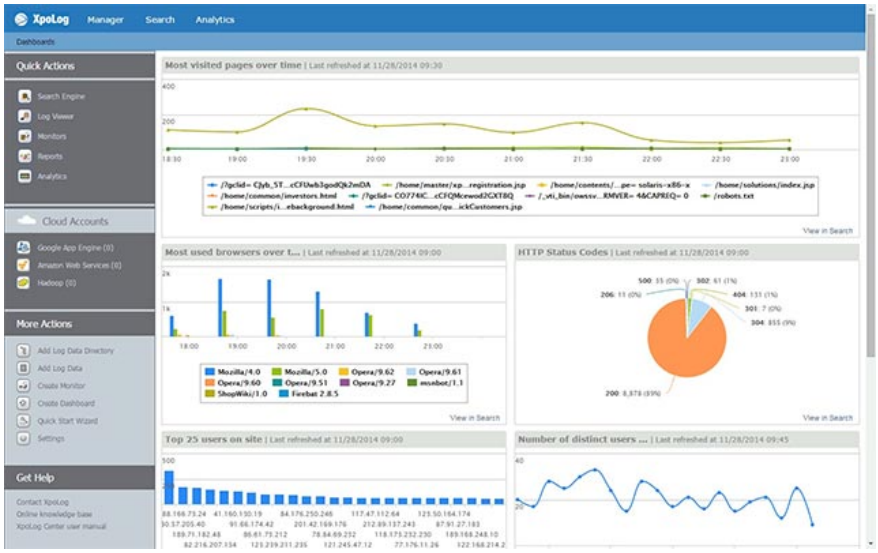
1. Supercomputers can completely detect cyber threats

Secure enterprise network space

1. Activity log analysis - XpoLog
2. Application and data protection - Imperva
3. Test penetration behavior - Metasploit
4. Preventing phishing attacks - Hoxhunt
5. Detecting fraud - Riskified
6. Develop network security investment strategy

Activity log analysis - XpoLog

Prerequisites before making any security incident response is that businesses must know exactly what is happening in their infrastructure. The good news is that all modern computer systems and digital devices have a flexible logging operation mechanism designed for many situations as well as data processing and processing processes. inside them. In general, diaries may reveal models and trends that are likely to be a sign of a breach of security or the penetration of malware into devices and systems.



1. Google: 2-factor authentication can prevent 100% of automated bot hacks

However, because the log files are basically 'repositories' containing information stored in plain text format, so manually analyzing log files can be a process difficult, very laborious and time consuming.

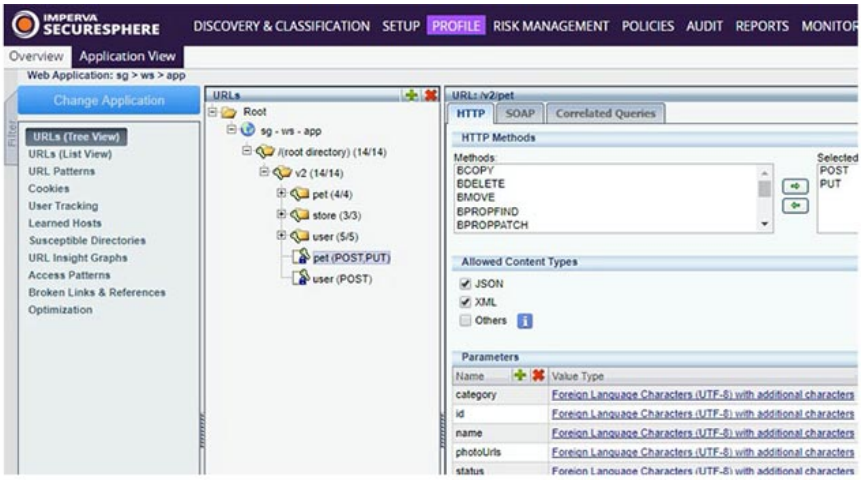
One way to effectively exploit logs is to use the log analysis support tool like XpoLog. The solution used here is simply to collect log files from various sources such as servers, terminals and applications in real time. After that, the application will mobilize the assistance of artificial intelligence (AI) to synthesize, analyze and evaluate the information stored in these log files, thereby identifying other alarm patterns. together. Detailed information obtained through the analysis process can easily inform the administrator of the status of the system as well as any issues that need attention.

You can download and try the XpoLog log analysis application here.

Application and data protection - Imperva

Before deciding to launch a targeted attack campaign, cyber criminals will continually explore the infrastructure of the business, so it is important to own the mechanisms that can prevent it. Instantly block malicious traffic from accessing key network resources such as web applications and databases . for the purpose of collecting information.

This requirement can be easily implemented through the use of web application firewall systems (WAFs) and data protection services.



1. Stack Overflow hits the hacker face, no significant damage is recorded

Imperva is one of the leading names when it comes to WAF service as well as in the mitigation and prevention of distributed denial of service (DDoS) attacks - which is also a popular form of network attack. most for businesses worldwide. Almost every organization and enterprise now maintains a hybrid infrastructure platform including on-premises devices and cloud components such as templates, storage and data warehouses.

Imperva's WAF can be deployed to protect the above resources. Basically Imperva will configure traffic and transactions to be done, while preventing traffic and malicious actions from entering these components.

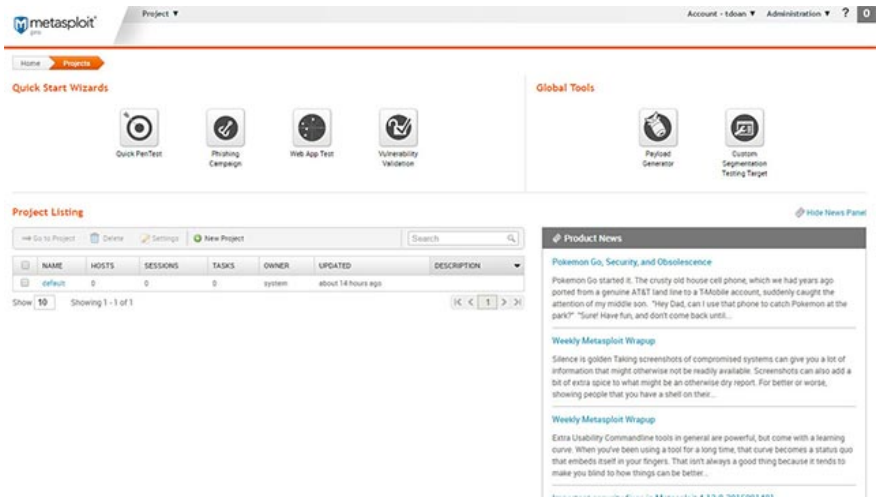
You can download and try the Imperva web application firewall system here.

Test penetration behavior - Metasploit

Integrating security tools into infrastructure is an important thing to do, but check to see if these tools work really well.

Again, businesses should not wait until the cyberattacks have actually happened before starting to find out if the security solution they have implemented before has worked effectively. No mistakes. It is an extremely negative, passive approach, in the way of 'losing new cows to make a cage' and does not really mean much in preventing a security disaster. In return, take the initiative to test your defenses according to the specific route, which is completely within the reach of your business.

System administrators can perform penetration testing using third-party frameworks such as Metasploit. This is an open source tool that can be configured to scan exploits and even deploy a payload on vulnerable systems.



1. Authentication tool on many enterprise VPN applications that are bypassed by hackers

Besides, Metasploit also has the ability to identify selective evasive tools, potentially breaking existing security measures. This application is currently available on popular operating systems such as Windows, Linux and Mac OS X.

Early detection of hidden vulnerabilities in security barriers allows companies to have the opportunity to overcome potential problems before a real attack takes place, helping to minimize the damage involved. to security.

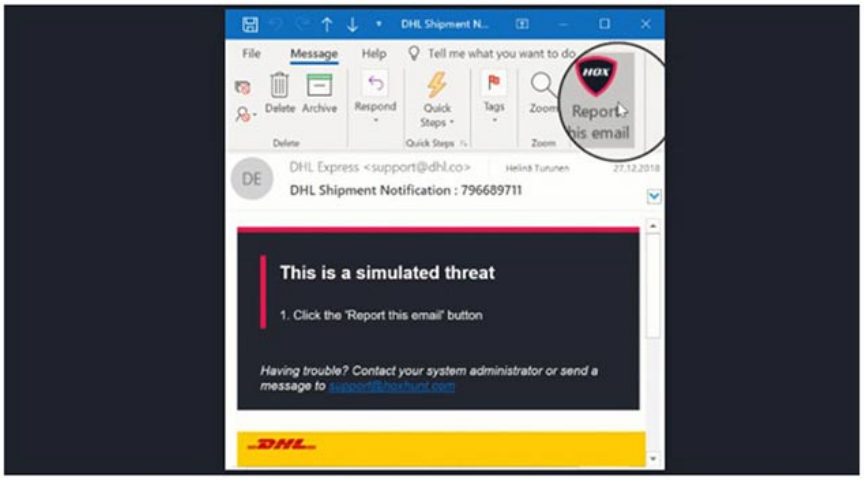
You can download and try the Metasploit penetration testing tool here

Preventing phishing attacks - Hoxhunt

Human factor is always the biggest link in every security hole on an enterprise network security system, this is a proven fact.

According to statistics, more than 90% of network security violations are found to originate from human mistakes. This is why cyber criminals are still actively using social engineering attacks such as phishing to infiltrate and take control of the infrastructure even though the most advanced defense systems have been Investment enterprises have not regretted their hands in the past few years.

Such attacks often target internal members of the network. Hackers will trick them into providing login information or installing malware into their systems to steal information. HoxHunt is one of the 'special treatment' tools for this problem. By guiding and assisting users to check whether the incoming email is a fraudulent message, or whether the website you are trying to access is a malicious website.



1. Insider attacks are becoming more and more popular and difficult to detect

In addition, businesses can also directly train and improve their ability to respond to real-life situations for internal employees by using phishing attacks. Hoxhunt's AI-based control tool even allows personalization of simulated attacks to accurately simulate how real-world attacks take place.

At the same time, users can report these attacks via a special plugin and they will receive immediate feedback on the level of completion of the test.

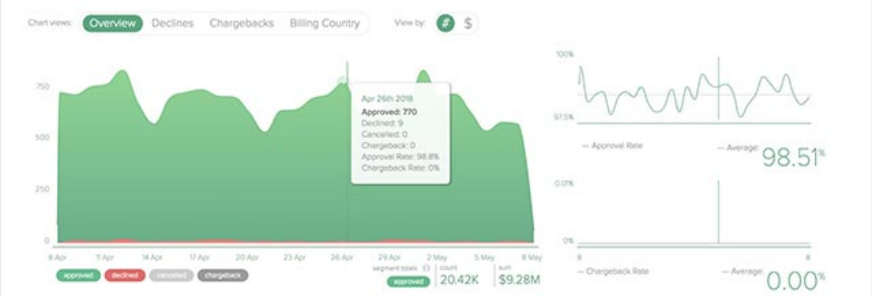
You can download and try the Hoxhunt phishing attack tool here.

Detecting fraud - Riskified

It may sound absurd, but not all cyber attacks seek to violate or steal information from companies. Another form of attack that businesses should especially note is fraud.

Hackers as well as scammers now have access to millions of records of valid personal and financial information that they have accessed from previous data violations. From there, it is easy to manipulate e-commerce channels of businesses, causing losses of up to billions of dollars at the global level.

In this situation, using third-party fraud detection security solutions will be the best option. Secure fraud detection tools like Riskified will provide you with comprehensive means to identify and prevent any fraudulent activity that may occur during online transactions.



1. [Infographic] How to recognize and prevent Phishing attacks

The method of operation is also very simple, Riskified uses AI (specifically machine learning) to analyze each transaction and only allow legal, qualified orders to be processed. In addition, this tool also provides automatic payment adjustments based on the customer's risk profile, bringing a variety of means for customers to verify the security of each purchase. they.

For example, a customer who owns a higher risk profile may be required to perform a few additional verification steps without completely rejecting the transactions.

You can refer to Riskified's solutions here: www.riskified.com/solution/

Develop network security investment strategy

An effective network security strategy requires businesses to pay attention to all areas, aspects that can be exploited by attackers. At the same time this will also require the presence of comprehensive tools and solutions to keep the system infrastructure safe from any potential situations.

However, before investing in security systems, businesses should also consider all relevant factors such as cost, level, and effectiveness (theoretically). Be very cautious when making these investments, avoiding the case of 'money loss, disability'.