MELBOURNE IT

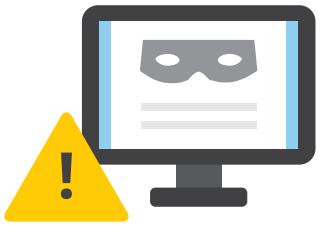
/ BROCHURE /

THE IMPORTANCE OF **MULTI-LAYERED WEB SECURITY**

By Melbourne IT Enterprise Services

MULTI-LAYERED **WEB SECURITY**

While the rapidly evolving internet connects modern businesses and organisations to their audience with greater speed and clarity than ever before, it also connects them to the denizens of the darker corners of the web. Therefore, the unfortunate reality is that if your business has an online presence, you are a potential target for the attentions of all manner of hackers and cybercriminals.



Fortunately, cyber crime awareness is growing at the business leadership level and enterprises of every size and scale are becoming painfully aware that they simply cannot afford to ignore the expanding threat landscape as it grows in size and sophistication. Unfortunately, while CEOs/CTOs and other business leaders understand that they need to protect their company against these myriad threats, too many exhibit a fundamental lack of understanding about current cyber security best practices and the most effective methodology to tackle threats before they ever come close to making a successful breach.

Current research suggests that the majority of IT security managers still exhibit an overreliance on their in-house defences to effectively protect them. The "fortress" mentality of creating a strong security perimeter on-site for the company's data centre still lives on, but the current threat landscape has emphatically proved – time and again – how ineffective this policy really is. Massive DDoS attacks can overwhelm even the most powerful on-premises hardware as it represents a single point of failure which can be hammered into inoperability by a tide of malicious traffic. Data theft attacks are becoming more difficult to detect all the time and without a series of proactive monitoring and detection tools it's only a matter of time before one slips past the perimeter.

In short, the data centre fortress is dead. On-premises solutions lack the power and sophistication to provide effective protection alone because they are reactive; they can only begin to combat the incoming threat after it enters the data centre, meaning that the damage may already be done. However, if a company's installed hardware works in concert with managed cloud-based services which live outside the data centre in order to secure, monitor and filter incoming traffic, then this multi-layered security strategy can proactively begin to protect against all manner of threats before they reach the company's infrastructure.

86% of IT managers from a recent IDG Research survey said that they felt either somewhat, very or extremely confident in their cyber threat defences. 77% of the respondents' companies utilise firewalls and 59% have intrusion detection but only 26% use cloud-based mitigation services to make a multi-layered cyber security approach.

The internet's threat landscape is evolving rapidly with 20,000-30,000 new malicious URLs being seen each day – that's a rate of one new URL emerging every two seconds. 80% of these malicious URLs are actually legitimate sites that have been compromised, making it more advisable than ever to use security solution providers who are handle global traffic in sufficient volumes to allow them to track emerging threat patterns.

THE MULTI-LAYERED APPROACH TO **COMBATING DDOS**

UNDERSTANDING ITS IMPACT

The threat of Distributed Denial of Service is receiving far greater levels of attention as the frequency and scale of such attacks have exploded during the past two years. Companies know that they can be targeted by DDoS and generally have a much better awareness of the nature of these attacks which utilise multiple nodes to spam their target with a tidal wave of malicious traffic at the network layer. However, too many IT security managers fail to truly count the ultimate cost of a successful attack by accurately measuring its potential impact on the company.

It's unsurprising that in most cases the affected company's IT department is most impacted by a successful DDoS attack. However, sales, security and risk management, operational logistics and procurement, customer service, marketing, PR and legal departments can all be adversely affected by prolonged downtime. Ultimately, depending on the size and scale of the business targeted, the total damages of such outages can measure anywhere from $5,000 to $100,000 dollars per hour as the company's operational mechanisms stall.

Along with loss of revenue, other costs can be incurred such as a loss of customer trust. This is often compounded by the loss or theft of consumer data as the most worrying new trend of attack is the use of DDoS to mask data theft attacks which are launched once the target's security systems are already engaged.

"We believe that with the costs for attackers decreasing and costs for businesses increasing, DDoS targets have broadened from financial institutions and government sites to any company that depends on its online channels, like online retailers and SaaS vendors."

– Marc Gaffan, CEO of Incapsula

COMBATING THE THREAT

As discussed preciously, any single point of failure device can be overwhelmed by the sheer volume of malicious traffic that a dedicated DDoS attack can bring to bear. The size of volumetric DoS and DDoS attacks has been growing exponentially and by 2020 Akamai predicts that the average DDoS attack will generate 1.5 Tbps of network traffic.

In order to ensure access to enough bandwidth to keep its servers up during an attack, companies can either install multiple redundant systems or utilise a cloud service provider's Content Delivery Network (CDN). CDNs are comprised of servers physically located all over the world in a distributed architectural format in order to provide the required bandwidth access as and when it's required. Unlike with the old fortress perimeter philosophy, an attack would have to overwhelm each one of these servers simultaneously in order to be successful.

CDNs offer the necessary DDoS protection but only require you to pay for the bandwidth you use, often making them a more economic alternative to installing multiple redundant systems to supply backup bandwidth. However, one important consideration is "Economic DDoS" a recent and insidious form of attack which targets companies protected by CDNs in order to drive up bandwidth usage and incur massive fees into the bargain. Therefore, it is vital that you check that your cloud provider offers capped bandwidth fees as part of its service level agreement – otherwise your servers will stay up during an attack but you may not be able to afford the resultant cost.

However, securing the capacity to withstand massive amounts of traffic is only half the battle when combating DDoS. It's also necessary to have the means to filter incoming traffic in order to separate and block the malicious requests while allowing legitimate traffic through. DDoS Mitigation Providers do exactly that by operating "scrubbing centres" to filter all incoming traffic before it reaches your data infrastructure.

Intelligent platforms make use of a globally distributed Web Application Firewall (WAF) in order to inspect every HTTP and HTTPS request bound for the target data centre. Malicious attack traffic is identified before being dropped or "scrubbed" while legitimate traffic is allowed to continue on its path. This stops attacks at the edge of the network space rather than relying on reactive security protocols to mitigate the damage of the attack once it has already breached the perimeter.

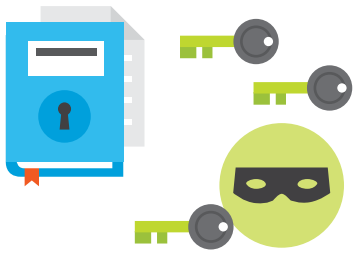
Through an effective combination of sophisticated equipment, technical rules and the direct intervention of human experts who are constantly familiarising themselves with new and evolving attack patterns, DDoS Mitigation Providers are equipped to offer a comprehensive protection solution which works in concert with a company's existing on-site hardware. Still, each business' data centre and assets are unique, meaning that there's no "one-size-fits-all" solution. The best DDoS Mitigation Providers offer an entirely flexible and scalable solution which allows the company to customise the defence rules for each online environment that they wish to protect. Done correctly, this can lead to an optimal security solution which balances the dual priorities of protection and ongoing site performance.

THE MULTI-LAYERED APPROACH TO **COMBATING DATA THEFT ATTACKS**

UNDERSTANDING ITS IMPACT

Businesses which rely on their online presence in order to operate are storing valuable data in greater quantities than ever before: customer contact details, credit and debit card numbers, all manner of private and sensitive data is housed within their servers and cybercriminals are well aware of its value. As the tools available to data thieves have become increasingly refined and powerful, their ambition has risen accordingly, with more audacious and damaging attacks being perpetrated with worrying regularity.

The impact of a successful data theft attack cannot simply be measured terms of the data that is wiped or stolen. It's true that the attack may incur significant immediate costs to the company as it becomes necessary to replace or upgrade the deficient security and storage hardware. However, for well-known businesses who suffer a publicised data theft attack, the damage done to their reputation is much more lasting. Existing customers may be encouraged to turn to competitors for more secure transactions and new customers will undoubtedly think twice before choosing an online retailer/service provider that cannot guarantee the security of their personal and financial data.

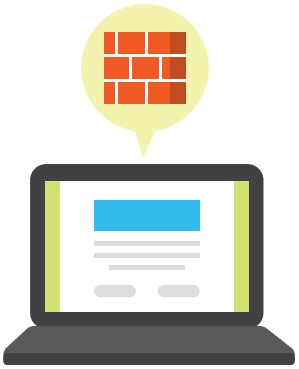


In 2011 Sony experienced a data theft attack where hackers stole the email addresses, birth dates, phone numbers, usernames and passwords of 1 million of its customers. Sony estimated its cleanup costs at a conservative $171 million, which involved 65 class-action lawsuits filed against the company by affected customers.

Between 2005 and 2012 six cyber criminals utilised sophisticated hacking techniques to steal more than 160 million credit and debit card numbers between them, targeting more than 800,000 bank accounts and penetrating servers used by the NASDAQ stock exchange.

In May 2014, 233 million eBay customers had their stored personal data stolen. Security experts roundly criticised eBay's response to the attack, citing delays in informing their customers of the breach followed by crashed servers as millions of customers tried to change their passwords as advised.

COMBATING THE THREAT



Whether the attack utilises SQL Injection, Remote File Inclusion or Local File Inclusion, it will most likely take advantage of vulnerabilities which are inherent at web application layer. This makes them significantly more difficult to detect as they are designed to blend in with legitimate application traffic in order to bypass traditional network-layer security tools. Companies can help defend themselves against such attacks by writing properly secure application code and patching all security software to keep it up to date. However, no matter how diligently your developers patch and code their applications with security in mind, it's always possible that a persistent hacker will discover the vulnerability they need to exploit in order to inject malicious commands.

As with DDoS attacks, front-end applications should be protected by security tools which proactively monitor application traffic and intercept illegitimate traffic at the network edge. WAFs are designed to perform deep packet inspection of HTTP/S requests and responses in order to block those which carry the hallmarks of an SQL injection/RFI/LFI attack. However, a WAF is only as good as its rules set, since a poorly configured WAF can either be too permissive and let attacks through or too restrictive, making it resource-intensive and hampering the performance of the protected sites.

Ideally, a fully-effective WAF should be configured with rules which identify well-known application attack patterns as well as emerging ones. Most solutions will adequately cover the former objective but many struggle to truly achieve the latter. No single online business with an in-house WAF can hope to remain aware of all emerging threat types, whereas many of the top cloud service providers handle vast daily traffic volumes and can therefore detect new attack patterns as they appear, swiftly developing effective WAF rules to block them before sharing their findings with their customer base.

In addition, a WAF should be flexible enough to be programmed with sufficient situational awareness to block suspicious activity patterns without overzealously blocking innocuous requests. For example, a generic Google search shouldn't be blocked whereas one which is specifically looking for info on web application vulnerabilities should. This is why IT managers of companies utilising a WAF should take the time to become familiar with its features and capabilities whether it is used as an in-house appliance or as part of a managed solution from a cloud service provider. By understanding the WAFs capabilities, the company can work with its service provider (if partnered with one) to configure an optimal rules set which accounts for the company's business requirements while covering its specific vulnerabilities.

"Most IT pros know that there is no silver bullet, and they don't put all their trust in a single security solution. The ultimate responsibility lies with organisations to determine their key assets, identify where vulnerabilities lie and design security that will protect them from attack and detect any breach."

SANS Institute – Layered Security: Why it Works

PROACTIVE **NOT REACTIVE**

PROTECTING YOUR BUSINESS THROUGH A MULTI-LAYERED SECURITY SOLUTION

Individually, the two major threats of DDoS and attacks that steal data should represent genuine cause for concern for companies which maintain any form of online presence. However, the threat runs deeper still, as underlined by the rising frequency of DDoS and data theft attacks which are being launched in concert by hackers looking to tie up security resources with DDoS before slipping in command code to steal their target data. This kind of devious innovation highlights the need for a comprehensive, multi-layered approach to online security if a company hopes to effectively protect its data and operational viability.

For those companies who understand the nature of the current threat landscape and the evolving capabilities of the hackers who have created it, an open and honest assessment of your security infrastructure should be the first step towards achieving effective security. With a firm grasp of the current risks most likely to affect your sites and applications, security managers need to decide how existing security controls can be best augmented in order to combat the threat.

Each business organisation will have a unique data centre configuration as well as a unique set of security priorities which will more often than not be constrained by budgetary considerations. This doesn't simply account for the initial cost of installing hardware, but rather the total cost of ownership, including the ongoing cost of maintaining the security system and/or utilising cloud service providers. In addition, managers of every online security solution need to consider its impact on the performance of the company's websites.

Therefore, it's imperative to find a solution which satisfies the business' need for optimal web performance while comprehensively providing proactive protection at the same time. Relying on the outdated "fortress mentality" can end up costing more in terms of installation and maintenance while still failing to provide the required tools needed to protect your data infrastructure. Contrastingly, a managed cloud service solution utilises a global network of analytical and defensive capabilities which work inline to constantly monitor and protect against all known and emerging types of attacks.

Concerted and coordinated cyber threats require an equally concerted security solution which combines the inherent strengths of multiple layers of defences. Stopping attacks at the network edge – or at the very least slowing them until they can be detected and mitigated – should be the ultimate goal of IT managers looking to procure a viable security strategy for their company.

"Sometimes DoS attacks work in conjunction with attacks on data, acting as a distraction while the hacker steals data. Dell SecureWorks Counter Threat Unit reported that a popular DDoS toolkit called Dirt Jumper was being used to divert bank employees' attention from attempted fraudulent wire transfers of up to $2.1 million."

– Brenner, Bill, Aug 2013

SOURCES

http://idgresearch.com/thwarting-ddos-attacks-with-cloud-defenses/

https://www.bluecoat.com/documents/download/d26767b2-d549-4a10-8002-8db194b79bb8/97040296-a8fe-40b4-b070-d190d0686652

http://www.securityweek.com/ddos-attacks-cost-40000-hour-incapsula

http://mashable.com/2011/05/26/sony-playstation-network-170m/

http://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948

http://www.telegraph.co.uk/technology/internet-security/10849689/eBay-hacking-online-gangs-are-after-you.html

http://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805

https://blogs.akamai.com/2013/08/DDoS-Attacks-Used-As-Cover-For-Other-Crimes.html

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

http://money.cnn.com/2012/03/30/technology/credit-card-data-breach/index.htm

MELBOURNE IT

ABOUT MELBOURNE IT

Melbourne IT Enterprise Services designs, builds and manages cloud solutions for Australia's leading enterprises. Its expert staff help solve business challenges and build cultures that enable organisations to use technology investments efficiently and improve long-term value. With more than 15 years' experience in delivering managed outcomes to Australian enterprises, Melbourne IT has been long associated with enabling success. Its certified cloud, consulting, and security experts repeatedly deliver results. This is why many of the brands you already know and trust, rely on Melbourne IT.

THE RIGHT SOLUTION IS MELBOURNE IT

melbourneitenterprise.com.au

1800 664 222 corporate.sales@melbourneit.com.au