/delivers/

WHITEPAPER

Evaluating The Cost Of A DDoS Attack

Businesses that choose to not protect their infrastructure don't just run the risk of a DDoS attack; they put out a welcome mat for attackers. DDoS attacks are becoming more sophisticated and destructive, and are on the rise. In a Ponemon Institute study, 65 percent of organizations had an average of three DDoS attacks between September 2011 and September 2012, costing each of these companies an estimated average of $3.5 million in downtime.[1]

In the same survey, 71 percent of respondents realize that anti-DoS/DDoS defenses specifically are important or very important.[2] But just how important are they to you? It should depend on what you're protecting. What's the cost of an hour of downtime to you, both in dollars and in value that doesn't easily carry a price tag like productivity or reputation? Your answers should determine the level of protection you need.

Considering The Cost Of Downtime

You are under siege and your website is down, transactions aren't processing or your your email won't send. Calculating potential loss is an imperfect science, but it's important to consider all of the aspects impacted by preventable downtime and the effects it has on your operations.

Potential Sales Lost

If you have an ecommerce website, it may handle a significant amount of your business transactions. Also, if you have an ecommerce business, your website represents all of your sales. A DDoS attack could devastate revenue, particularly if your site becomes unavailable during peak traffic or transaction times.

Top ecommerce companies experience on average a loss of $1 million for every minute of downtime. In 2012, 476 of these top sites collectively experienced a revenue loss of $1.8 billion. While this number reflects losses from downtime due to multiple factors, it shows just how costly just a few hours of downtime can be, whether caused by a DDoS attack or not.

It's also important to take into account the average and potential downtime when considering your possible

2012: TOP ECOMMERCE SITES GET HIT HARD BY DOWNTIME

1,102,919
total minutes
of downtime

3,421
average minutes
per company

$866,038,469
in total
lost revenue

$1,890,913
average lost
per company[3]

revenue loss. The Ponemon study identified the average amount of downtime following a DDoS attack as 54 minutes.[4] However attacks exceeding 12 and even 24 hours are common.

Revenue is just one aspect of dollars lost. The Ponemon study stated the average cost for each minute of downtime was about $22,000, which recognizes not only lost revenue but also lost traffic and diminished end user productivity.[5]

Hard-To-Measure Costs

Revenue losses due to downtime can be fairly predictable. As shown in the aforementioned statistic from Ponemon, dollar values can be assigned to productivity as well, but it's more difficult to measure. You need to think about the IT operations, security, help desk, and business continuity professionals who would be consumed by trying to manage the downtime and get operations back online. Depending on the DDoS target, line-of-business productivity can be immobilized as well.

Outside the walls of a business is no prettier. Sales and transactions cannot be processed during downtime, but the damage doesn't stop there. First time visitors are unlikely to return to a site that is down. Existing customers can be turned off and could look to a competitor for immediate needs, never to return.

With social media as the immediate medium in which people report and engage about news, share high profile site outages, and air general unhappiness about service providers, your reputation and brand value can be damaged before you even know what's happening. Plus if you're a business that has service level agreements for uptime, you may be subject to penalties.

But wait, there's more! A DDoS attack may be used to misdirect attention and IT staff from a more serious security breach, such as the stealing of intellectual property, sensitive business information or customer data. These data leakages carry their own hefty tangible and intangible price tags.

1 minute of downtime costs $22,000 when factoring in lost revenue, lost traffic, and diminished end user productivity.

"Cyber Security on the Offense: A Study of IT Security Experts," Ponemon Institute and Radware, November 2012.

Weighing The Cost Of Mitigation

Based on your potential damage, some level of protection is a must, but security requires some planning and investment. If you worry because your security budget is a bit snug, you're in good company; only 44 percent of survey respondents believe that their security budget is sufficient for mitigating most cyber attacks.[6]

Think about approaching security by weighing proactive cost against potential loss and decide how much you're willing to risk. Doing nothing is not an option. Otherwise, the risk of a DDoS attack becomes a guarantee.

Security Infrastructure

Many of today's DDoS prevention tactics have found their way into IT infrastructure. The 2012 Neustar survey found a 10 percent increase over 2011 in the use of firewalls, switches, and routers. While these tools ward off DDoS attacks to protect you, they can actually increase network congestion by bottlenecking traffic. Intrusion detection systems cause the same problem, but they are helpful in defending against compound attacks in which DDoS is used to draw attention away from a data breach.[7]

9 percent of survey respondents use on-premise hardware to mitigate attacks,[8] but this approach has limited value when dealing with attacks like DDoS amplification. This can easily consume all of a company's network resources.

So how much will an onsite security solution run you? The expected and unpopular answer is that it depends. The cost will vary greatly on the hardware, software, and services in use. An entry-level offering can cost a few thousand dollars, and the price goes up—as high as six figures depending on complexities and features.

Deciding On The Right Level Of Protection

You have a lot of factors to consider when deciding how much risk you are willing to open your business to.

Attack Frequency: Companies in one survey were attacked three times on average in one year.[9]

Attack Length: Attacks can last hours or even days, depending on how long it takes you to mitigate the traffic and what the attacker has for resources.[10]

Attack Probability: Industry matters. In 2012, retail attacks increased by 144 percent, with 39 percent of all surveyed retailers having been attacked, along with 41 percent of ecommerce businesses. And 44 percent of financial services organizations were attacked in 2012. But no one is immune. In 2012, 35 percent of companies experienced a disruptive attack.[11]

Dyn

WHITEPAPER

There are many DDoS-specific solutions available to shield yourself against attacks, but if you're feeling overwhelmed and ill equipped, you're not alone. Only 29 percent of organizations believe that they have the in-house expertise needed to combat hackers and other cyber criminals.[12]

The good news is that you don't have to handle the risk on your own. There are various solutions, like managed DNS, available that can take the burden off you and protect against DDoS attacks, leaving you to focus on strategic projects that benefit the business. Managed DNS is delivered as a service, so there's no need to buy hardware, install software, or hire more IT personnel. You gain all the benefits of enterprise-class DNS protection without the work or upfront costs.

Want to hear how we can protect you? Give us a call or email now.

ATTACKS LASTING LONGER THAN 24HRS BY SECTOR: 2012[13]

Travel:40%

Retail: 33%

IT:28%

Finance: 26%

Telecom: 21%

1, 2, 4, 5, 6, 9, 12 "Cyber Security on the Offense: A Study of IT Security Experts," Ponemon Institute and Radware, November 2012.

3 Internet Retailer's 2013 Top 500 Guide

7, 8, 11 "Hope is Not a Strategy: 2012 Annual DDoS Attack and Impact Survey: A Year-to-Year Analysis," Neustar, April 2013

10 "Develop A Two-Phased DDoS Mitigation Strategy," Forrester Research, May 2013. While researching for this report, Forrester spoke with John Jellema, global security product manager at Verizon Business, who gave insight into how costly extended outages are.

13. "DDoS Attack Survey," Neustar. http://www.neustar.biz/enterprise/resources/ddos-protection/ddos-attacks-survey-whitepaper#.Us8Ly2RDvq8

dyn.com sales@dyn.com +1 888 840 3258 150 Dow Street, Manchester, NH 03101 USA