DDoS Risk Assessment

A guide to assessing your vulnerability to distributed denial of service (DDoS) attacks

A self assessment guide from Bell

Determining your DDoS risk profile

As distributed denial of service (DDoS) attacks become increasingly prevalent, having a strategy in place to protect your digital assets and infrastructure is key. But it needs to be the right strategy, tailored to your organization's specific IT security risks and requirements.

In fact, not every organization needs to invest in comprehensive, ultra-robust DDoS protection. Before committing IT spending to a security solution, take a few minutes to answer the questions in this assessment. Doing so will help you start a focused conversation about your DDoS risk profile and the level of protection you need, which will put you in a much better position to zero in on the right solution – and the right security provider – for your organization.

How visible is your organization online?

- Do you have a large online presence?
- Are you a well-known national or international brand?

If so, you're more likely to be higher up on an attacker's list of potential targets – and more likely to require an in-depth DDoS security solution.

While some attackers are motivated by financial gain (via extortion or ransom), others are simply looking for fame and notoriety. Taking down the website of a news agency, movie studio, online retailer, video game publisher, government department or other high-profile organization is an easy way for attackers to generate publicity and capture the attention of their peers.

Are you in a high-risk industry?

- Do people rely on your organization's online services?
- Are you in a line of business that is susceptible to negative feedback?

Your DDoS security needs depend greatly on the type of business you are in. While no industry is immune to the possibility of a DDoS attack, certain kinds of organizations are more likely targets than others – and require a higher level of DDoS protection. The following graphic shows which industries are targeted most frequently by DDoS attacks, and the contributing factors that make them potential targets.

Industries most targeted by DDoS attacks[1]

1.

Gaming

- Games are evolving more towards online multiplayer, where even the slightest downtime can disrupt the user experience
- Many games need to be online at all times, creating a single point of failure that attackers can exploit
- Some attacks are launched to protest changes made to a game and others are just for notoriety

2.

Software and Technology

- As more solutions are dependant on cloud-based technologies, such as Software-as-a-Service (SaaS), any outages can significantly impact users
- Centralized distribution of software introduces a single point of failure that attackers can exploit
- Attackers commonly target this industry with web application attacks[1]

3.

Media and Entertainment

- News agencies and movie studios are often targeted due to their high visibility
- Hacktivists may shut down a news site to protest the types of articles it publishes

4.

Internet and Telecom

- Attackers usually hit an ISP to knock offline the services it provides to their real targets
- ISPs that host a high number of sites (or high-value sites) are at greater risk

5.

Financial Services

- Banks, insurance companies and payment providers – and even small credit unions and brokerage houses – present an opportunity to extract and monetize financial information
- With the security team distracted by the website outage, the attacker can potentially breach the internal network, install malware and steal customer data
- Attackers commonly target this industry with web application attacks[1]

6.

Education

- Common targets include email servers or online services for submitting work, entering grades and managing admissions
- With the rise of 'DDoS-for-hire' services, any disgruntled student with a credit card can quickly and easily launch an attack

7.

Government

- Not every attacker is politically motivated: some want to publicly shame the government by exposing its lack of online security, while others are looking for notoriety[2]

8.

Retail

- Downtime of an e-commerce store directly impacts revenue and reputation
- Cyber attacks can be distractions for other attacks – e.g., ransom attacks or large data breaches
- Consumer information on retailer databases makes them an attractive target
- This industry suffers the highest proportion of web application attacks[1]

---

[1] Akamai. *Q1 2016 State of the Internet - Security Report*. Retrieved from https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2016-state-of-the-internet-security-report.pdf.

[2] Radware. *2015-2016 Global Application and Network Security Report*. Retrieved from https://www.radware.com/ert-report-2015/.

How important is your web presence to your business?

- Do you conduct real-time financial and other customer transactions over your web infrastructure?
- Does your business depend on providing a consistent, reliable online experience to your customers?

If you answered "yes" to either question, DDoS protection is highly recommended – even if you're not a big national brand – as downtime is costly.

In fact, if you're a smaller organization that relies heavily on the Internet for e-commerce or other customer transactions, it will be much harder for you to bounce back from the lost revenues and negative customer perceptions that come with a prolonged DDoS attack.

What would be the impact of an attack on your business?

- What would be the cost of any amount of website or server downtime?
- How much would it cost to recover from an attack?
- How would an attack affect your brand and reputation?

If your e-commerce website is taken offline, you'll suffer immediate consequences in lost sales. And the longer it takes your IT team to reboot your applications and servers, the more opportunities will slip through your fingers. Getting a everything back up and running at full capacity could take hours or even days. Is your business capable of weathering that storm?

Taking into account lost revenues and IT labour costs, 35 percent of North American IT security decision-makers say it would cost between $10,000 and $100,000 to resolve a DDoS attack, and 31 percent identified it would cost over $100,000.[3] And that doesn't include the potential damage to your brand image and reputation. In a world driven by social media, bad customer experiences could affect your ability to attract and retain customers long after the attack has been resolved.

Talk to Bell

Bell offers a number of managed and professional security services that can help you perform a more thorough assessment of your security requirements, plan your strategy and implement a DDoS solution that's right for your organization.

Contact your Bell representative to learn more about how our experts can provide the guidance and insights you need to protect your network and your business.

---

[3] Forrester Research. (2014). *Protecting Customer Experience Against Distributed Denial of Service (DDoS)*. Retrieved from https://business.bell.ca/shop/enterprise/forrester-network-ddos-security-white-paper.