Enterprise Strategy Group™

BRIEF

MARCH 2025

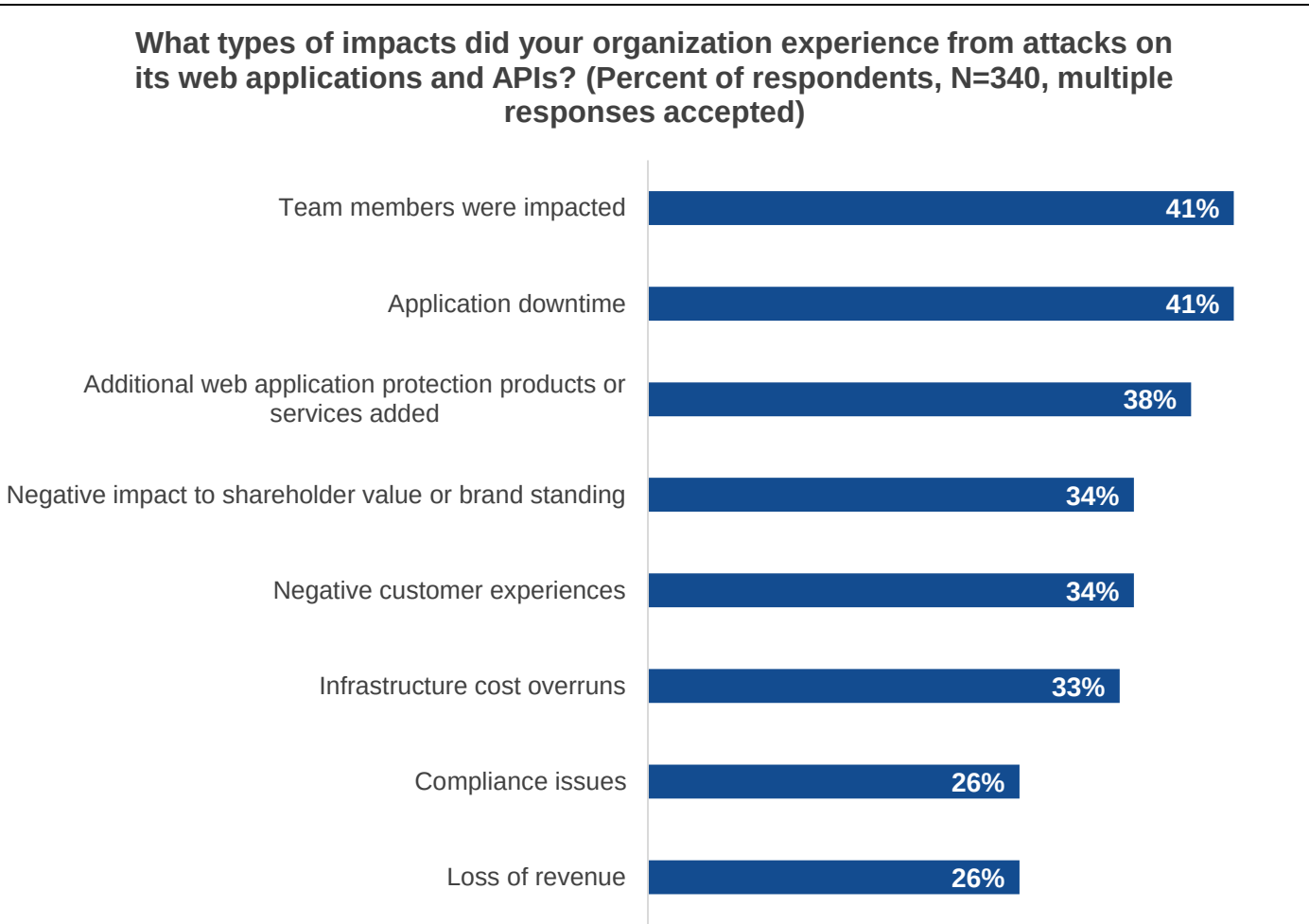
C/side Highlights the Growing Risks Around Client-side Web Application Security

John Grady, Principal Analyst

Overview

Protecting web applications from attack is a key priority for nearly any business transacting or connecting with customers online. A key reason why is the broad range of adverse impacts organizations can face when application attacks are successful (see Figure 1).[1]

Figure 1. Impacts From Web Application and API Attacks



Source: Enterprise Strategy Group, now part of Omdia

[1] Source: Enterprise Strategy Group Research Report, *Trends in Modern Application Protection*, July 2022.

Some of the most notable include:

- **Poor customer experience.** At a minimum, an attack can affect application availability. While this can be a minor inconvenience for customers, if sensitive customer data is stolen the ramifications can be much more significant.
- **Compliance issues.** The Payment Card Industry Data Security Standard (PCI DSS), Digital Operations Resilience Act, and General Data Protection Regulation are key regulations which apply to many types of businesses. Failure to comply can lead to fines, bad publicity, and even customer lawsuits.
- **Financial repercussions.** Whether due to a direct loss of revenue due to downtime, impact to shareholder value, or the additional costs incurred following an attack, impacts to the bottom line can be significant.

Client-side Attacks Pose a Unique Challenge

Web application security is often overly focused on server-side attacks and defenses. Ensuring that attackers cannot inject malicious code in the application itself, access data they are not entitled to, overload the system with fraudulent requests, and so on. Yet as applications have become more distributed, interconnected, and reliant on the use of third-party scripts, the issue of preventing browser-side supply chain attacks has risen to the forefront.

These types of attacks often target the third-party services an application relies on, hijacks them, and exploits a user's device or browser, one example being the attacks targeting the Magento ecommerce platform that gave rise to the ongoing attacks dubbed Magecart across other similar platforms. When customers access an application using a compromised third-party script and begin to input their information, the malicious script running on the client browser captures the data and sends it to the attacker. Another common client-side attack involves a third-party exfiltrating the session token of a user, enabling the third party to log into the account of the impacted user. More exotic attacks like client-side crypto-mining, crypto wallet theft, and running client-side botnets to attack others websites are also on the rise.

It can be difficult for security teams to ensure visibility and control over these third-party scripts for a few reasons. The scripts are typically managed by front-end engineering, legal, or marketing, are numerous (especially on larger ecommerce sites), and are updated frequently. But getting ahead of this issue has become critically important, as PCI DSS version 4.0.1 puts additional requirements in place specifically around client-side security.

Traditional web application security vendors such as Imperva and Akamai have offered solutions in this area, and application owners can craft a content security policy to manage how browsers interact with scripts and other application components. However, a handful of standalone vendors are offering purpose-built tools to address this issue. One that has recently come to market is c/side.

C/side Client-side Protection

The c/side solution runs as a proxy. Customers add a small script from c/side to their webpage, which redirects any third-party script traffic through c/side's proxy before going to the user. The proxy operates only for third-party scripts and not the entire page, which helps ensure performance is not affected despite traffic being redirected. In fact, because c/side also caches scripts on their edge, it can deliver them faster and improve performance in some cases.

While compliance is a significant driver for this type of solution, c/side has focused heavily on security. The proxy model ensures that known scripts are constantly monitored for any changes leading to malicious activity, as well as providing insights into unknown scripts that might be operating on the webpage. The c/side solution uses both threat intelligence and artificial intelligence to analyze scripts via its proxy. Analysis is also run asynchronously, so if something does initially get through it can be identified as new information becomes available and blocked in future instances.

C/side is available on the AWS marketplace, helping customers to retire platform credits. The solution is available in three versions:

- The free tier supports one domain and basic functionality and support.
- A Business version is available for $99/month/domain which extends protection to include source analysis, a longer script history period, and automated blocking.
- Enterprise pricing is also available, which adds audit logs, as well as additional support resources, reporting, and dashboards, including a purpose-built PCI DSS dashboard view.

Conclusion

Client-side attacks stemming from hijacked third-party scripts are an underappreciated, but significant issue organizations should be addressing. In fact, any organization transacting online must have client-side protection in place when the transition period for PCI DSS version 4.0 ends and becomes mandatory. But beyond that regulatory motivation, it simply makes business sense. There are countless examples of companies that lost customer trust due to cybersecurity incidents of one kind or another. Once lost, that trust can be difficult and expensive to rebuild. By ensuring that the third-party scripts running on their website are legitimate and benign, security and web teams can help protect their brand and their customers' sensitive personal data.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com