Don't let outdated security leave you red-faced on Black Friday

By Simeon Tassev

17 Nov 2021

November has become a peak month for online shopping and combined with the rapid growth of e-commerce during the pandemic, this could be a recipe for cybersecurity disaster. While many online retailers have worked hard to improve security over the years, others were hasty in their move to online, and security vulnerabilities may still exist. Now, as retailers rush to be present for two of the most significant shopping days of the year, it is more important than ever to tighten security ahead of time and not leave this for the last minute.

Image source: Karolina Grabowska from Pexels

Online vulnerabilities

Globally, there have been significant updates to major e-commerce platforms to address inherent security vulnerabilities, and there has been a push for online retailers to migrate to the latest versions. This has gone a long way toward improving security for the online shopping experience, but there is still a lot of work to be done.

The challenge around online shopping is the fact that actual physical payment cards do not need to be presented, which opens up the potential for card fraud. Payment Card Industry Data Security Standard (PCI DSS) compliance is mandatory, and this has improved security in-store with better systems and processes, and practices like end-to-end encryption. However, the reality is that many retailers still view e-commerce as a spin-off of their physical presence and are not treating cybersecurity with the necessary business priority.

An attractive target

Online shopping, particularly on peak days like Black Friday and Cyber Monday, presents an opportunity for cybercriminals to steal large numbers of card details and other personal information. It is a lot less risky than attempting to do this in-store, where the risk of getting caught is much higher and the payoff significantly lower. With a successful

exploit, cybercriminals could potentially steal millions of cards before the retailer even suspects an issue, which from a business and brand perspective is hugely damaging.

While e-commerce is growing, both locally and across the world, retailers need to approach the security problem with far more attention and due care. As uncertainty around the pandemic continues and the appeal of Black Friday and Cyber Monday grows in the country, it has become imperative to ensure security is adequate.

Multi-layered security is critical

PCI DSS compliance is essential from a payment card security perspective, but it is not sufficient on its own. Retailers need a multi-layered approach that starts with the basics, including web application firewalls, and up to date anti-virus and anti-malware software. In addition, it is critical to make use of a reputable, reliable e-commerce platform, and ensure the latest version is running, to prevent security vulnerabilities. Making sure the site uses secure HTTPS protocol and not just HTTP, which is cleartext and therefore vulnerable, and securing the site with SSL certificates, is vital.

Aside from the technology, a solid security strategy must also be tested regularly, otherwise, data security cannot be guaranteed. This involves more than vulnerability scans and penetration testing because by their very nature e-commerce sites must allow users authorised access otherwise they cannot shop. Testing simulations need to determine how the system is protected from authorised users who are not privileged – in other words, a customer who is authorised to use the site, but should not be able to access any backend information such as payment details. Ensuring the site is set up correctly is paramount.

While online retailers need to be present on Black Friday and Cyber Monday, rushing into it without the proper focus on security could end in crisis. It is imperative to carefully consider security and not get caught up in the last-minute rush, which might result in a breach that could cause more damage than the increased sales are worth.

ABOUT THE AUTHOR

Simeon Tassev, MD and QSA at Galix