Consumer-Facing Websites Surpass the Enterprise in Security

by Nikitas Magel December 16th, 2014

Now, fully two weeks after the solid kickstart of Black Friday and Cyber Monday, the holiday shopping season is full swing. And more than ever before, a significant amount of that shopping is done online—a practice that's booming. This season alone, as Forrester Research predicts, Americans will spend $89 billion online, 13 percent more than last year.

While this is welcome news for the retail industry, the growing number of online transactions means that increasingly greater volumes of sensitive customer data are being transmitted—and possibly exposed. Which means that online retailers have a lot to be concerned about.

But ironically, with respect to website security these businesses are in much better shape than their enterprise counterparts. As reported in a study commissioned by Neustar and released last month, the analysis firm Quocirca found that website security tends to be significantly more robust and is much more widely practiced among consumer-facing businesses.

In essence, enterprise websites are at much greater risk for breach and compromise.

Specifically, the report found that, compared to their business-to-business (B2B) counterparts, consumer-facing businesses are significantly more likely to…

- **Invest heavily in online security measures.** They're more likely to implement cutting-edge protection against distributed denial of service (DDoS) attacks, fraud, and advanced cyberthreats. Enterprise organizations, on the other hand, rely more heavily on dated technologies, leaving them more vulnerable to sophisticated attacks.
- **Dedicate a higher proportion of budget to online resources.** They tend to invest far more in improving the customer experience online. Related to these efforts is the gathering of metrics used to match shopping behaviors to revenue and gauge customer loyalty.
- **Hire external resources for site protection.** They outsource both infrastructure and security, allowing them to dedicate more internal resources to improve the customer experience and increase conversion rates.

The study has caused ripples throughout the technology media, both stateside and abroad, putting business-facing organizations on notice. In response to the findings, Neustar's senior vice-president and technologist Rodney Joffe stated that "lessons can clearly be learned from consumer-facing organizations operating at the sharp end of cyber space."

The difference in online vigilance arises from the simple fact that consumer-facing organizations have been compelled to develop a more robust online presence as a matter of commercial survival. And that's for two reasons. First, business-to-consumer (B2C) relationships are more tenuous than B2B ones. The retail landscape nowadays is such that customer loyalty can rest heavily on the experience that shoppers have with a particular website. If that experience fails to meet their expectations, they'll easily abandon a potential transaction in favor of one with a better user experience, especially given the sheer number of choices there are for retail shopping. Business users, however, are much more limited in their choices of products and services and by the overall procurement process of their organizations. Secondly, payment for B2B transactions is often delayed by lines of credit, whereas consumer transactions are more immediate, putting B2C organizations under the watchful eye of regulatory agencies.

And so, even as consumer-facing websites experience a huge surge in online transactions during the holiday season, they're better prepared than their enterprise counterparts in minimizing or even preempting cyberthreats. As awareness of this reality grows, B2B organizations could potentially experience increased targeting by a hacker community looking to take advantage of their vulnerability for the easier kill. These businesses would do well to take heed. As Joffe has pointed out, "The key to successfully protecting your online domain is not to be able to outwit your cyber attacker; it is about outperforming your competitors with better protection."

ddos protection, it security, retail