The festive rush: when security can't be allowed to slow down retail

By Anton Jacobsz

23 Dec 2014

Festive season in South Africa is traditionally a time of big spending, but it's also a good opportunity for fraudsters and cyber criminals to strike and prey on consumers who are in holiday mode and businesses that are focused more on keeping the shelves stocked than being on guard.

Anton Jacobsz, Managing Director of Networks Unlimited, says that during the December holiday season, the risk of phishing attacks disguised as festive greetings or seasonal special offers may rise. Year-end bonuses make credit card fraud and theft all the more attractive to criminals. Hackers with a grudge could launch an attack on an online store to far greater effect at this time of year. And in the rush of dealing with hordes of shoppers, staff mobile devices loaded with sensitive information and access to company systems could get lost or stolen. Recent data breaches in the retail industry have also exploited vulnerabilities in in-store wireless networks.

Anton Jacobsz

Most targeted industry

"Retail is one of the industry verticals most targeted by cyber criminals, according to Fortinet research, and the chaos of the festive season presents more opportunities than usual for cyber criminals to strike. Clearly, this is no time for retailers to let their guard down when it comes to IT security," says Jacobsz.

"However, traditional IT security measures can have certain downsides. Crucially at this time of year, traditional firewalls could slow down transaction processing time and thus slow retail operations, causing slower-moving queues and frustrated shoppers. Often, retailers opt for low cost branch solutions which are not scalable and may also be cumbersome to manage in a constantly-changing threat landscape."

Another traditional low-cost security approach is to bring all the data back over a private wide area network (WAN), such as an MPLS VPN, and implement multiple central security systems at the data centre. But this too can make data integration and reporting a tedious process and ineffective for rapid response to new vulnerabilities.

Ensure maximum security

Jacobsz says that in a competitive environment, retailers need to ensure maximum security while still delivering high performance for an excellent customer experience. And they must do so cost-effectively. In-store networks must deliver low latency and high performance for continuous credit card processing and point of sale connectivity, especially during peak transaction periods such as the festive season rush. Next-generation firewalls are needed to thoroughly inspect large numbers of transactions, without degrading performance.

Multi-Threat Security Systems should feature an intelligence-based structure that aggregates and correlates information from a variety of unified threat management sources, with a unified platform that can analyse user behaviour in internal and external sources, and immediately red flag any anomalies, without slowing processes down.

"By moving from traditional IT security to the next generation of unified threat management solutions, retailers stand to not just cut costs, but reduce their risk of financial losses and reputational damage, while at the same time improving the level of service they are able to deliver - even during the busiest shopping season of the year," he says.

High performance solutions

With Fortinet's Unified Threat Management security solution, a retail organisation with hundreds of stores can quickly deploy and operate comprehensive high performance security solutions to all endpoints for a fraction of the costs of traditional solutions and stand-alone appliances.

The combination of world-class network security and central management allows a retailer to have robust security for network resources, no matter where data is stored or accessed. Retailers can easily deploy and centrally manage security appliances throughout the distributed network, from kiosk to superstore. This helps supporting multi-channel operations and innovative services such as customer access, as well as providing a high security posture and the tools to maintain compliance with PCI-DSS.

The increased functionality of a single platform for unified threat management with the flexibility of integrated Wi-Fi, 3G failover, traffic aggregation and high performance ASICs provide unmatched performance and agility at each store.

ABOUT THE AUTHOR

Anton Jacobsz is the Managing Director of Riverbed distributor Networks Unlimited