BIZCOMMUNITY

4 ways retailers can prepare for cyberattacks this upcoming holiday season

By Byron Horn-Botha

22 Nov 2021

Retailers have become the main target for cybercriminal attack activities, driven by the exponential growth in online shopping, the pandemic and the need for physical distancing. In short - retailers are primary targets.

Byron Horn-Botha, Arcserve Southern Africa lead: channel and sales | image supplied

A ransomware attack hit 44% of retail organisations in 2020, and many paid a very high price. The average cost of recovery from a ransomware attack in the retail sector was nearly $2m, according to the *State of Ransomware in Retail 2021*. The costs included downtime, people time, device cost, network cost, lost opportunity, and ransom paid to recover encrypted data—this translates into an average of $147,811.

As we approach Black Friday and the year's busiest shopping season, the bad-actor community is gearing up to launch a new wave of attacks, which is not jolly news for retailers. It will be a make-or-break season for many. Now they face the possibility that a cyberattack could put them out of business even if sales go well.

This mounts pressure on retailers to secure their data and protect the personal information of their customers. If you are a retailer, here are four ways you can keep the bad guys at bay and have a happy and profitable holiday season.

1. Get the right data storage

Retailers need to manage and protect a lot of data, from credit card numbers to email addresses to invoice information. Having the right data storage solution enables you to protect critical data, even if you're a victim of a ransomware attack.

Your organisation should look for an immutable data storage solution that safeguards information continuously by taking snapshots every ninety seconds. You can still recover your information even if ransomware does sneak through and your data is overwritten. Because these snapshots are immutable, there will always be a series of recovery points, ensuring that your data will be safe.

2. Strengthen your weakest link

Firewalls, endpoint protection, email security, etc., are all crucial. Backup and recovery are also a critical part of the overall IT security solution. And if it's not done correctly, it will be your weakest link. Having a comprehensive backup and recovery plan lets you protect your data if disaster strikes—not just a cyberattack but also basic incidents like a power outage, snowstorm, or hardware failure.

Your backup and recovery plan should include a simulation of business disruption to assess your strategy. It should also include regular testing of your backup images so you can resolve potential issues before they occur. Retailers with a recovery plan are more likely to escape maximum damage and permanent data loss.

20% of companies in SA have no cybersecurity plans for holidays or weekends, study finds

19 Nov 2021

When it comes to data protection, you should hope for the best and prepare for the worst. Having a solid plan in place can ensure your business remains at the top of its game during the all-important Black Friday and holiday shopping season.

3. Understand that not all data is created equal

Data tiering is critical for retailers. The approach involves moving less frequently used data, or less vital data, to lower storage levels for cost, recoverability, and availability. The premise is that not all data is created equal, so it's essential to have different sets of policies based on how critical the data is and how quickly you need to access or recover it.

Yes, it's good to have your quarterly results at hand. But if you lose access to that information for a few hours or days during the height of the shopping season, it won't hurt your sales. However, if your business' price list is compromised or your delivery addresses are not accessible, it could have an immediate and profound impact on your business. That's why it is so important to prioritise your data and understand the value of each piece of data.

4. Protect your data in the cloud

Many retailers operate in the cloud. If that is the case for you, it is essential to understand that cloud security is a shared responsibility between you and the cloud provider—and that the sharing is not divided entirely equally. You - not the service provider – are primarily responsible for protecting your data in the cloud. Retailers need to make sure they read the small print in their cloud service contracts. Top-tier providers like Microsoft Azure, Google Cloud Platform, and AWS typically secure the core infrastructure only. But when it comes to securing data, that responsibility falls squarely on the shoulders of their customers. Retailers who fail to grasp this simple fact are much more likely to suffer a data loss.

You should be aware of your responsibility, ensure that you have appropriate protections in place, and regularly test your ability to recover from data loss if it happens.

You can have the best technology from a prevention standpoint - but even with this in place – the bad guys can still get slip in unnoticed and wreak havoc.

ABOUT THE AUTHOR

Byron Horn-Botha, lead: Arcserve Southern Africa Channel and Partnerships.