Holiday Season Is Prime Time for Hackers & Ransomware Demands

Posted by Mike Heumann, December 19, 2022

Businesses are prime targets for cybercriminals during the holiday shopping season. Think about it – most retail companies make the majority of their revenue in November and December (try to find a parking space at the mall during those months!). Hackers know this, and they also know that companies will pay off ransomware attacks during these months for exactly that reason. Historically, attempted ransomware attacks increase by roughly 30% during this time, as reported by Darktrace. If making your year's revenue means keeping (or getting back) the operation of your point of purchase systems (for instance), paying ransomware becomes an easy choice for most businesses.

This problem is also made worse by the fact that most retail-related businesses are exceptionally busy during this period. The Global Risks Report released by the World Economic Forum found that 95% of cybersecurity threats that people have faced have in some way been caused by human error. In addition to staff being exceptionally busy, they are also thinking about the holidays themselves, as well as being generally more tired. Unsolicited emails during the holiday season also increase substantially, giving cybercriminals a greater chance of launching successful phishing attacks. Given that most targets of phishing emails open the emails 70% of the time, the likelihood of a successful attack goes way up during the holiday season. Finally, computer networks tend to be under intense strain due to the increased traffic during the holidays, making the potential for network penetration significantly higher.

In addition to observances for year-end holidays, some organizations elect to shut down for more extended periods of time. For example, nearly half (44%) of U.S. employers responding to Lockton's 2021 HR Trends Survey reported that they closed their doors for Christmas Eve in 2021, and 5% were closed from Christmas through New Year's Day 2022.

Employees scramble during this timeframe – with end of the quarter pressures, end of the year work wrap-up, shopping while shipping windows still meet holiday deadlines, plus colder weather which

contributes to the desire to stay under the covers longer each morning (and avoid all of those other pressing stressors.) There is a labor shortage and the people who are present are maxed out. Hackers are aware that there is more valuable data to pounce on during the holidays, so a successful attack would be more rewarding. With increased shopping, retailers have more consumer data. It's no wonder that 24% of attacks target retailers.

Add to this the normal exploits like remote desktop protocols, misconfigured ports, and recent Microsoft Exchange vulnerabilities, and you have a recipe for potential disaster.

ThriveDX explains that an increased risk of cyber attacks during the holidays doesn't mean that your organization should sit back and do nothing and offers the following to protect your business from from cyber threats:

- Training employees to raise awareness about cyber threats to minimize human error
- Identify flaws and vulnerabilities in all your organization's connected devices
- Update all your software
- Add an extra security layer to your enterprise's email accounts
- Make customer service more accessible to address concerns swiftly
- Regularly test your cyber defenses
- Have a robust contingency plan

Stay alert to avoid getting your business hacked, shut down, or otherwise disrupted. And Happy Holidays!