INSIGHTS

Cyber made simple.

one brightly cyber

RANSOMWARE ATTACKS GROW

BY JAY BORDEN

Ransomware is a scourge that keeps growing. Researchers report that for the first time ransomware payment totals broke $1 billion. That figure makes it a larger business than most SMEs, Small and Medium Enterprises.

The ransom, even for a small business, can be thousands of dollars or more. Then there are the costs associated with recovery; getting your systems back up and running, the business lost until they are back, the negative reputational impact, regulatory filings, etc. Don't think paying the ransom will instantly restore your systems, it won't. Even if the key given by the attackers works, and it doesn't always, it still takes time; time you can't serve customers, place orders, process payroll, etc.

Despite their belief that they are too small to attract attention, SMEs are key targets. Why, because SMEs tend to be resource constrained in money and people. Cybersecurity teams are small or non-existent and budget is limited. Outsourcing IT or cybersecurity is a popular approach. However, it is not a panacea. You can outsource the function, but you cannot outsource the responsibility, meaning you still have final responsible for protecting information.

Cybersecurity tools are often seen as the answer to cybersecurity woes. But tools cannot protect against everything. If they did breaches would be far less common. Please do not misunderstand. Tools are necessary and certainly do help against many things. But they do not work against everything.

People are the cause of over 80% of breaches. Falling for a phishing email or phone call is a common way for attackers to penetrate. Tools will rarely stop these types of attacks.

MFA, Multi-Factor Authentication offers protection beyond a password and can be very effective. But be sure to choose a phishing resistant type of MFA.

onebrightlycyber.com
(888) 773-1920

RANSOMWARE ATTACKS GROW

CONTINUED

Think of ineffective MFA methods as adding a second lock to your front door. Then leaving both keys under the mat.

Many types of attacks start with phishing emails and a user clicking a bad link. The link goes to a website that looks real but is a copy of the one you want. You are asked to enter your credentials. Now the attackers have them. If MFA is used, the attackers also have that.

Using those credentials, the attacker logs onto your servers or applications. They will look for ways to reach other servers or applications, and user devices to load malware or ransomware onto as many as possible. They may install a backdoor, a way to continue to access things even if a password is changed.

Replying to an email or a text signals to your systems that you trust the sender and the systems will not be as concerned as before. It may be as simple as a text that says “hi how are you doing? Or “are you there?”

What can you do?
First train everyone in your organization how to spot phishing emails and not fall for them. Test their understanding by sending phishing emails and see who takes the bait.

Next is to use phishing resistant MFA or passkeys. Passkeys are a successor to passwords that create unique codes for each system or application. They are tied to your system. If the login request comes from your system, an authorization request will be sent. If you approve, you are in. If you don’t, you aren’t. Approval can be through a unique pin, face scan or finger print, or other biometric feature.

Remember, attackers don’t rest. With each new way of blocking them, they look for ways around it. You can’t rest either. Staying up to date on attacks and new security methods helps you stay safer.

Most important is to educate your users and test them regularly. So many attacks start with people falling for a phishing email, phone call, or other method.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.