SECURITY ON A SHOESTRING

COST-FREE WAYS TO PREVENT CYBERCRIME

BY JASON BROWN

CISO, Merit Network

Cyber threats are on the rise – putting businesses, dollars and real lives in grave danger. Regardless of an organization's size, most companies deal with securing personal information, computer networks and connected devices to conduct daily operations. As cyber attacks grow in frequency and sophistication, associated costs to mitigate these attacks skyrocket. According to Gartner, the worldwide security market reached $75 billion in 2015. This spending is expected to increase in 2018 to $101 billion and reach an estimated $170 billion by 2020.

How can businesses with minimal IT and cybersecurity budgets keep up with today's demands? Fortunately, there are a number of cost-free solutions that organizations can adopt to make a positive impact in their security program.

1. CHANGE YOUR PASSWORD

As much as one-third of all data breaches and cyber attacks can be attributed to weak or out-of-date passwords. These breaches can be accomplished through password cracking programs, phishing attempts, theft and the illegal buying and selling of personal data. It takes more than 200 days, on average, for a victim of cyber attack to notice the breach.

Unsafe passwords, such as '123456' and 'password' are among some of the easiest credentials to crack and still heavily used to this day. However, creating unique and long passwords for each account can prove difficult to remember. Password managers, such as LastPass or KeePass, can help users create and safely store credentials that are difficult to breach.

An added security measure of multifactor authentication processes should be considered at the organization level. Multifactor authentication (MFA) is a system that prevents data theft by requiring more than one source of credentials from a user or employee before they can access your data. For example, organizations could install a push-notification app, like Duo Security.

2. SEE WHAT THE BAD GUYS SEE

What exactly do the "bad guys" know about your network? Search engines like Shodan and Censys gather enormous amounts of information about your company's network and publish it online. Through sites like this, hackers can locate your organization's potential vulnerabilities. For example, a hacker could discover that systems on your network use a weak SSL cipher which can be used extract sensitive information. These search engines also identify open internet-based cameras and baby monitors that can be used for spying purposes! Conversely, this information can be used by a business to help identify and patch weaknesses before a breach happens.

3. KNOW YOUR USERS AND TRUST YOUR DEVICES

Over time, some organizations develop what is referred to as "a hard outer shell and soft in the middle." This refers to instances when companies deploy firewalls and other security services which protect the perimeter of the network, while ignoring the security of internal systems.

The proliferation of cloud-based services and BYOD (bring-your-own-device) practices have increased vulnerabilities with the "hard outer shell" security approach.