Slithering Cyberthreats

cyber security technology

Summary: With the explosion of IoT devices comes increased cyber risk for banks. Guidance from the government has been released to keep organizations safe. We have the main takeaways.

A study in Ecology and Evolution Journal finds a potentially scary situation. Researchers testing DNA from pythons in FL have found 3% of the snakes carry genetic markers that could create a "super snake" interested in moving from the swamps to higher dry ground. That is a potentially risky situation slithering around.

Some technology researchers might say yet another risky situation developing in and around banking might be the Internet of Things (IoT).

Look no further than a report jointly issued by the Department of Commerce and Homeland Security. It warns of the risks created by the increasing number of mobile devices and their interconnectedness. As community banks strive to protect customer information and use vigilant cybersecurity measures, keeping these guidelines in mind is key.

Share information and best practices. First and foremost, the report emphasizes the importance for businesses and service providers, which interact with the public through mobile devices, to have a broad understanding of the importance of shared efforts to protect against botnets. As part of that, the report recommends that organizations should work together to foster the adoption of best practices and share information about any compromises.

Monitor and communicate. Among the specific steps that community banks and businesses can take is to make sure they are closely monitoring the point where their networks interact with customer networks, such as cloud providers. As part of this effort, community banks should also make sure they have the capability to deal with realistic amounts of malicious traffic and ensure their customers are aware of their efforts in these areas.

Always identify the source. Since everything from devices in the IoT to data center servers can be compromised by botnets, there are multiple points of entry to manage. Further, since it can be difficult to keep all systems updated, community banks need to take the time to properly identify the source of incoming electronic communications. Make sure not to be spoofed or unwittingly help botnet controllers disguise their real locations on a larger scale. Legacy systems can add to the problem, given that security measures can be out of date or in need of patching. Pay extra special attention here, if you are using older technology.

Continuously educate on new risks. Another step to take is to make sure IT staff has the opportunity to continuously stay educated about new risks. Staying connected to the industry and law enforcement for relevant updates is critical.

Know the vulnerabilities of new devices. Community banks should also be aware of the risks of incoming IoT devices used by both employees and bank customers. Ericsson predicts there will be more IoT devices in use than mobile phones by the end of this year. You read that right, so be prepared, because risks are spreading quickly. Educate customers and employees to avoid security issues, as new IoT devices enter the market.

While the ultimate goal is for technology systems to automatically report any security breaches, we are not there yet. Until then, be especially diligent monitoring your systems and staying in-the-know about new mobile devices and their risks, to avoid the tight squeeze of incoming cyberthreats.

WEBINAR: NAVIGATING THE GLOBAL NEEDS OF YOUR CUSTOMERS

September 20 | 10:00-10:30 AM PT **Webinar Registration**

As your customers expand their business across borders, you will want to expand with them. Join us for a free webinar where we will discuss the benefits of using international services, as we highlight foreign wires and foreign cash letters. We will also discuss digital cash clearing for Canadian checks.