BIZCOMMUNITY

Improving cyber security is vital in the digital age

By Joy Mali

28 Oct 2016

Nearly everything in today's world goes through a computer system at some point. With sensitive consumer information, financial data, and more stored in networks, criminals have quickly discovered they can cause more damage with a single cyber-attack than with anything else.

You've seen the number of data breaches that seem to occur on a regular basis, and if you collect and store the same type of information that you see hackers going after, you must realise that your system could come under attack too. In fact, it may have already been hacked and you just haven't seen the signs of it yet.

In today's digital age, it's vital that you improve your cyber security before an attack happens. Here are 10 different ways you can do so.

1. Understand your system vulnerabilities

Computer networks are complex, which means their security vulnerabilities are too. With so many different areas to protect you need to know exactly which ones hackers are likely to target and where your weakest points are. Sit down and critically evaluate your system, noting which areas are the most likely to be attacked and where you really need to improve your security. You may need to hire an outside professional to truly give your system a critical once-over or to even try to hack your network to see where your problem areas are.

2. Gather intelligence

You can make use of various security analytics in order to gain a large amount of predictive insight. This insight provides you with the information necessary to know where your system may be vulnerable, but it goes beyond that. It gives you insight and an understanding into your system as a whole, and that can help you determine what information about your network is the most useful. You may also be able to get a better idea of why a hacker has targeted your business or network, which in turn will help you prepare better defences.

3. Assume an attack has already occurred

Start out by assuming you've already been breached in some way. Many companies don't actually start seriously defending against cyber-attacks until they have been attacked already, but by then it's too late. The damage is done. So instead of waiting, assume you've already been attacked. Create a plan to counter these attacks and implement it as soon as you can.

4. Use account management for additional protection

One area of weakness in your defence is user accounts. It can often be easy to break into one of these accounts and gain access to your entire system. Using various challenges and identity authentication can help reduce the risk of this occurring. Also create user roles that limit access to only what that employee needs to have access to. For example, someone who has no need to deal with the company's financial information should not have access to the folder where it is stored.

5. Develop a strategy for data loss prevention

It can be difficult to protect your data if you don't have a data loss prevention strategy in place. These strategies help you identify your sensitive data, put a plan in place to monitor it, and decide how best to protect that information. This includes the data you're currently using and the data you may have stored on computers, servers, and in the cloud. Remember, though, that your strategy may need to be somewhat flexible because you never know what will occur during a real cyber-attack.

6. Realise mobile devices bring both benefits and challenges

Mobile devices are everywhere now, and chances are just about every one of your employees is using a smartphone these days. You're not going to be able to prevent these devices in the workplace, but you can help control them. You can instruct employees on how to best secure their own devices and put protections in place on your network to make certain only those authorsed to access your Wi-Fi can do so.

7. Use intrusion prevention and detection software

Using an intrusion prevention and detection software will allow you to see who is in your network and what they're trying to do. You'll be able to see any unauthorised user and follow their attempts to break into your system or you can immediately remove their network access. But network intrusion protection does more than that. It will also alert you to your own employees if they attempt to access data they should not. If a user account repeatedly attempts to do so, it can be a sign that that account has been hacked.

8. Be proactive in your defences

While the court system is still trying to decide how prosecuting some cyber-attacks should be done, companies are dealing with these issues every day. You don't have to wait until there's a strong legal doctrine for protecting your network, though. You can be very proactive in your defenses, creating ways of keeping hackers out of your network by using the right methods and strategies.

9. Use defensive deception techniques

Defensive deception techniques are ways of turning a hacker's tools and methods back on them, making it harder to break into your system or more time-consuming. Many hackers are looking to score quick and easy data for financial gain, so if you make breaking into your system require more work, many will give up and move on to an easier target. By using defensive deception, hackers may believe that they are being attacked and hacked back, which will often be enough to scare them off.

10. Work with an expert

Finally, remember that your team is very close to your network, which is both good and bad. They understand all of its quirks, but they may also not realise where it has security issues. Bringing in an external expert can help you get a better view of your network, including areas that need more protection that what you've given them. These experts can attempt to break into your system in a simulated cyber-attack, which is often very helpful in determining which of your current security measures work and which are only partially successful.

ABOUT JOY MALI

Joy Mali is a certified digital analyst who helps online businesses to perform better on the web with best solutions & advice. Her content is featured on many mainstream sites & blogs.
- Improving cyber security is vital in the digital age - 28 Oct 2016

View my profile and articles...