CaroMont Health

Cybersecurity for Small Businesses

Guidance and Education from CaroMont Health's
Information Privacy and Security Office (IPSO)

Ed Brown, Director of Technology Systems

Small businesses are integral to the US economy

- The Small Business Administration defines small businesses as private companies that employ fewer than 500 people.
- About 99% of businesses in the U.S. are considered small businesses.
- Small businesses employee about 50% of workers in the USA.
- Small businesses are less likely to have designated information security teams and other resources big companies can afford, but still face the same risks.

CaroMont Health

If you think you are safe because you are “small”, think again...

- 58% of malware attack victims are categorized as small businesses.
- In 2017, cyber attacks cost small and medium-sized businesses (SMB) an average of $2,235,000.
- 92.4% of malware is delivered via email.
- 90% of small businesses don’t use any data protection for company or customer information.

CaroMont Health

Types of Cybersecurity Attacks

- **Socially Engineered Phishing**

  End users are tricked into downloading, running malware or giving their ID and password. Common types include: Phishing, Spear Phishing, Whaling, Pharming, Google and Dropbox Phishing

- **Ransomware**

  All data on infected devices is encrypted and “held ransom” by the bad guys. Common types include: WannaCry, CryptoLocker, CryptoWall, Petyas, Bad Rabbit, SamSam

- **Drive-by attack**

  Malware is spread by the bad guys finding insecure websites and planting malicious script or code on the site. People who visit the site get infected without ever clicking or downloading anything.

CaroMont Health

And there's more!

- **Denial of Service (DoS) or Distributed Denial of Service (DDoS)**

  Bad guys overwhelm a system's resources so it can't respond to service requests. Common types of attacks are: botnets, ping-of-death, smurf and teardrop
- **Exploiting Unpatched Software**

  Bad guys take advantage of known security flaws in operating systems and popular applications. Equifax breach in 2017 happened because they did not fix a known security flaw in an application they use.
- **Social Media Attacks**

  Social Media platforms are leveraged to do things like install software, access user contacts, location and activities. If your employees are using social media on their work devices, those devices are vulnerable.

CaroMont Health

Strategies for Security

- **Know where your important data is located.**

  Knowing where your critical business or customer data is physically located is the first step to being able to protect it and is also required by some regulations like privacy and payment card.

- **Backup, backup, backup!**

  Your data is the most important part of your computer system. Hardware that is lost, stolen, destroyed or made inoperable by malware can be replaced, your data cannot. Consider keeping your backups in another location, protected from fire, theft or other harm if possible.

- **Test recovery from backups.**

  Verify that you can get your data back BEFORE you really need to. Regular testing of backups by restoring and verifying data not only gives you confidence that your critical data is backed up, but also gives practice restoring from backup so if you are trying to figure it out during an emergency.

CaroMont Health

Strategies for Security

- **Keep your patches and anti-malware application(s) up-to-date.**

  Bad guys exploit known vulnerabilities with their malware. You might be able to automate some of the updating to make it faster and more convenient, but even if you have to do it manually, closing a security hole is worth it if it keeps malware out of your system or prevents it from being able to act.

- **Know what access people have to your data and keep it minimal.**

  Keeping track of your system users is important to protecting your system and data. Obviously removing access belonging to an unhappy former employee is important, but any unused account can be hijacked and used by bad guys to get your data or infect your system. Don't make it easy for the bad guys by giving everyone access to everything.

- **Watch what you throw away.**

  Old computers and even printers can have data on their hard drives, Throwing out paper with company information on it can be stolen by the bad guys and used to get information to make phishing emails look more legitimate and therefore be more successful.

CaroMont Health

Strategies for Security

- **Change all the default passwords.**

  Leaving default IDs and passwords in applications and on hardware like routers, switches and firewalls makes it easy for bad guys who get into your network to access your equipment and make changes to install their malware.

- **Educate your employees.**

  Train your employees on what to look for in today's cyber threat arena. For example, employees being able to recognize phishing email and NOT clicking on items in the message is critical in protecting a business.

- **Use policies to set expectations and define consequences.**

  It may seem like everyone should know to do certain things or not do others, but spelling it out in policies makes sure everyone has the same understanding. Detailing consequences of acting against policies helps employees understand the gravity of the situation and helps you as an employer treat everyone fairly in tense situations.

CaroMont Health

Questions/Comments

CaroMont Health

References

- 5 Cybersecurity Statistics Every Small Business Should Know in 2018
  https://blog.barkly.com/small-business-cybersecurity-statistics-2018
- 10 IT security risks that small businesses can't afford to ignore
  https://www.networkworld.com/article/2358151/network-security/network-security-10-it-security-risks-that-small-businesses-can-t-afford-to-ignore.html
- Small business cybersecurity risks for 2018
  https://www.pandasecurity.com/mediacenter/business/cybersecurity-risks/
- The 5 types of cyber attack you're most likely to face
  https://www.csoonline.com/article/2616316/data-protection/the-5-types-of-cyber-attack-youre-most-likely-to-face.html
- Cyber threat is huge for small businesses
  https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/

CaroMont Health