Five Ways to Boost Your IoT Security

The Internet of Things has created a new challenge for companies trying to keep their network secure. As the points of entry into a network increase, so does the attack surface, giving an attacker more opportunities to probe for vulnerability. In fact, Symantec's 2018 Internet Security Threat Report revealed a 600 percent increase in IoT attacks between 2016 and 2017. So here are five ways your company can boost their IoT security and help defend their borderless networks.

1. Start with the end (user)

Every year reports appear about company network security breaches. Often this is because an employee, or other end-user, didn't understand their company's security procedures or they used an easy to guess password. With so many extra devices on your network ideally, you need a dedicated IoT security policy. End user IoT devices are often consumer-grade like personal routers, music speakers, or other similar types of personal devices. If these devices are connecting to the corporate network they are subject to corporate

security policy and need to either be isolated completely or managed by the security policy of the company to ensure they are adequately secured.

Your policy needs to be easy to understand so all your staff will know what they must do. Organizing regular staff training will help keep everyone up-to-date and it will also help your staff, and other end-users, understand how, and why, you are protecting their data and the company's data.

2. Defend the Perimeter Network

The network perimeter is critical to the security of your network, especially when you are dealing with the IOT devices. It's important that best practices are followed when designing and implementing your security policy for an IoT based network, paying special attention to things like device authentication to the network, device network communication controls, and device logging. Ensure when possible that you are using strict authentication and authorization policies for your IoT devices, as many of these devices lack hardened operating systems and are often very vulnerable to attack. Ensure that sufficient logging of device access and network communication is in place as well to provide adequate detection capability of anomalous behavior so that it can be mitigated quickly before it becomes a major issue. When feasible ensure that you are implementing modern security inspection of IoT traffic as well: application-based rules, inspecting all traffic and rules for blocking particular websites, ensuring specific protocols behave according to standard rules (HTTP, DNS, Industrial Protocols, etc.)

IoT devices will be accessing the web in most cases more often than any other resources. This is particularly true when the IoT devices you are dealing with are personal devices like BYOD mobile phones and tablets. It's important that your content policy is sufficient enough to protect this attack surface as well. Often times BYOD users bring these devices back onto the corporate network or share data between these devices and their corporate assets, enabling possible compromises between the machines to be brought inside the network. When it comes to content control, it may not be the obvious sites, such as gambling or porn sites, that are the riskiest. In many cases, seemingly benign sites like local news sites, etc. are actually hosting ads that have been compromised and in fact delivery mechanisms for malware. It's important you can detect these attacks in this "gray" area of the content you are supporting. If the security on the websites your staff visit isn't good enough, the site could be compromised and your network could be at risk. As more devices connect to the network, especially with employees working remotely, the further your network perimeter expands. And the more complex it becomes to keep it secure and prevent threats finding 'holes' in the perimeter they can exploit.

A penetration test of your perimeter network is a good idea. Unknown devices can be logged, monitored

and the necessary actions taken according to your security policies and procedures.

3. Multi-layer endpoint protection

Hackers are always on the look-out for easy targets, so put obstacles in their way. How you do this will depend on your network. One way is risk-based authentication. When a user tries to access a secure part of your network, it decides whether they are a high or low risk. And then either allows them to access that part of the network or blocks them and alerts you about what happened.You could also use encryption keys to hide the identity of an IoT device. Or use digital signatures for devices so they can be identified on the network. Regular device auditing is also important, as your network perimeter expands, each new device needs to be secured. In the future, isolation solutions could help prevent web-based attacks. These work by creating a ‘space’ between the web and your end-users and increase endpoint protection.

4. Look beyond the obvious

Any device that can connect to the internet could be hacked. And it isn’t always the most obvious devices that hackers target. The Mirai botnet in 2016 was used to create a huge Dedicated Denial of Service attack. And one of the IoT devices they used were IP cameras running with their default settings.Other devices such as air quality monitors, printers, smart lights, thermostats, and sensors are at risk as well. As well as connected coffee machines or vending machines. Also look at devices that connect remotely to your network, you may have staff accessing the network for information they need. In fact, anything that connects to the network is a potential risk. So, an audit of every device that connects to your network can help identify at-risk devices.

5. Make data protection a priority

Data is often what hackers are looking to compromise. And the European Union’s General Data Protection Regulation could change data protection around the world.

All data, whether it is being sent over the network or stored, should be encrypted. SSL encryption, data encryption algorithms, and biometric access can all be used to protect data. In fact, a multi-layered and tailored approach works best.

A dedicated server for sensitive data, with strong security, can prevent data from being shared by mistake. A data audit may find data you no longer use. Providing it’s legal to do to so, you can then delete that data so it’s no longer at risk of being stolen. If you have employees sending, for example, work reports to the

network from mobile devices that data also needs to be secured. This is another example of how your network perimeter is expanding because of IoT.

In the future, artificial intelligence and blockchain technologies could be the basis for the next generation of data security.

The Internet of Things offers many advantages to companies. However, IoT devices mean the network perimeter is now faster, borderless, and highly distributed. Sophisticated technologies such as distributed firewalling and DNS-based security are important as your corporate firewall can't 'see a remote devices actions and activity. Getting this mix of technologies right is critical for the security of your network. So, if you need expert guidance, NWN can help.

Our experts can find the ideal solution for your company. For example, they can show you how Varonis Edge works and also offer you a free trial. As its name suggests, this product helps detect perimeter attacks including stolen VPN credentials and DNS attacks.