Businesses

DDoS

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a [denial of service](https://searchsecurity.techtarget.com/definition/denial-of-service) for users of the targeted resource. The flood of incoming messages, [connection](https://searchnetworking.techtarget.com/definition/connection) requests or malformed [packets](https://searchnetworking.techtarget.com/definition/packet) to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

Why this is concerning?

This is concerning because it means the attacker has access to the devices that are infected and the hacker could try to gain access to your network that way. For the most part DDoS infected devices will not change the activity they are meant to do. The device might be slightly slower but for the most part it is an undetectable difference. It is possible that due access to the network through the infected device it could spread to others on the network infecting them as well.

This is a link to give more information on why DDoS attacks are a big concern. It is written to promote a product, I do not know enough about this product or its competitors to say if it is good choice or not. The information on the page is accurate when it comes to the magnitude of the threat and is corroborated by many other articles.

<https://www.corero.com/blog/870-the-rise-of-iot-botnet-threats-and-ddos-attacks.html>

How to prevent this

* Do systematic reboots of your devices some malware will be uninstalled in the reboots.
* Make sure all factory passwords have been reset, not all the devices will have a password that you can reset so that is a on going concern.
* There are systems that monitor IoT devices to see if the traffic in and out is normal. Those monitoring systems have a high success rate in finding infected devices.

Cons

The cons are that each device would have to have a unique strong password which would be difficult to keep straight with as many devices as companies have. Devices that monitors your system can still make mistakes and infected devices could go undetected. The monitoring device could lead to a false sense of security. There would be a cost in implementing this in the sense that the system to motor your IoT devices would be high but changing passwords and rebooting devices is simple work and the cost of that would be low.

Ransomware

Ransomware is a type of [malware](https://techterms.com/definition/malware) that prevents you from using your computer or accessing certain [files](https://techterms.com/definition/file) unless you pay a ransom. It often [encrypts](https://techterms.com/definition/encryption) files so that they cannot be opened.

<https://techterms.com/definition/ransomware>

Why is this concerning

Companies are targeted because they have the money to pay the ransom easily and they don’t have time for the systems to not be functioning well. When the devices that control locks, heating/cooling and other vital systems to companies are ransomed there is no choice in many cases but to pay. If they do not pay then they would have to buy all new equipment, also if they don’t pay in a certain amount of time the ransom could go up or all data could be wiped from the devices.

<https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/>

How to prevent this

The best way to prevent this is to make sure that it is as hard as possible to access your devices.

* The passwords are strong and unique for each specific device.
* Make sure it is not possible for devices to download off of the internet.
* A system that monitors the traffic going in and out of the devices would help. It would alert if there was any unusual traffic happening with the devices which could point to people trying to access it and download ransomware.

Cons

Ransomware is a tricky attack because once it gets in your device will be encrypted and there is nothing you can do but pay. All defenses are about keeping out the virus because if it gets in then it is too late. Most other viruses you can get rid of once it had infected a computer. The con of all of these approaches is that it will take constant monitoring and checking to be sure nothing has tried to access the device. Even then the devices might still be infected, it is hard to protect against attacks such as this. The cost of all my recommendations is very little in comparison to if any of your devices gets ransomed. Companies would have to pay for a monitoring system and put in the man hours to make sure the passwords and settings are how they should be. It is still less expensive than paying the ransom in a lot of cases.

Man-in-the-middle

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. https://en.wikipedia.org/wiki/Man-in-the-middle\_attack

Why this is concerning

Man-in-the-Middle is dangerous because if the data is not encrypted on the IoT device before it is sent elsewhere then the hacker could read all the data being sent. That might not seem to important because who cares the thermostat is set to 68 but it gets more concerning when the key pads send what the updated key code is. Or the data shows the office is empty. Devices can give away information that by itself doesn’t seem to important but there are sophisticated algorithms that can draw very accurate conclusions from the data that would not be expected. It is also concerning because once the hacker has access to the network they can cause other problems as well.

<https://www.scmagazineuk.com/billions-bluetooth-devices-vulnerable-mitm-attacks-no-user-action/article/1474116>

How to prevent this

Best way to prevent man-in-the-Middle is to make sure that the network that device is communicating over is secure.

* Make sure the network is encrypted.
* If possible buy only devices with built in encryption. If the data is encrypted it would protect against what the hacker can see.
* Run scans of your network to be sure that only authorized devices are accessing it.

Cons

The cons to this is that you cannot add encryption to the devices, they have to have come with it. It is also hard to detect if there is someone monitoring the communications between devices and the scans of the network could not be on a set schedule they would have to be random. The cost of implementing this is very little due to the fact that routers come with the ability to encrypt. But it could be increased if the devices that come with encryption are more expensive

Spoofing

Spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

https://techterms.com/definition/spoofing

Why this is concerning

If there is a clearly open door onto a network such as an insecure IoT device then it is not hard to convincingly masquerade. It would be a very simple way for an attacker to gather data or send out data without anyone being aware something is wrong with any of the devices.

https://www.iotforall.com/iot-security-concerns-preventing-iot-hacking/

How to prevent this?

The best way to prevent

* Have authentication methods such as TNC ( trusted network control) which will authenticate each device every time they want to connect to each other. When a device is being spoofed it is hard for networks to be able to tell the difference so with authentication it will catch a spoofed device because it will not know the authentication key. TNC protocols will make sure that the device is who it claims to be before letting data flow between them which will lower the likelihood of spoofing.

Con

Authentication slows down a system because the devices have to do more than they are meant to also there are plenty of IoT devices that are not able to use complex authentication protocols. It will slow the network due to all of the authentication checks and not all devices will have the capacity to do the most secure checks. There is a high cost to this approach because the software is expensive and it could slow down a network.

Physical Tampering

When a hacker is able to access your device in person and tamper with it, possibly adding malware to it. Once an attacker has physical contact to a device it is very easy for them to download malware on to it. Most devices aren’t equipped to prevent against remote attacks much less physical tampering ones.

Why is this concerning?

Because with these viruses the creator doesn’t have to worry about how to get into the device remotely. The entire attack is focused on infecting the device and accomplishing the goal that the creator has in mind. With viruses like that it is easier to make them more malicious because they are custom made to be in your specific environment. IoT device tend not to be seen as high-risk points like computers because they aren’t directly connected to private company information. They are a risk though because the devices connect straight to the network.

<https://danielelizalde.com/iot-security-hacks-worst-case-scenario/>

How to prevent this

To prevent this the easiest way would be to make sure that the devices you have are

* Remove IoT devices from public locations such as lobbies or conference room that are accessible to people working outside your company.
* Another way to prevent this is to be sure that once the IoT devices are updated the newer models replace the old ones.

Cons

If a hacker is working hard enough to make a targeted attack based off the entry point of a IoT at your specific company, it will be difficult to keep them out of the system. Most networks have a lot of very weak entry points it is just a matter of finding the correct one. This is a medium cost solution because it requires money to update devices and move them out of public areas. After that though it doesn’t require much thought beyond making sure the models are up to date and only people who are supposed to be near the devices are.

Eavesdropping (Remote recording)

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference or fax transmission

https://searchfinancialsecurity.techtarget.com/definition/eavesdropping

Why is this concerning

This is concerning because through this method of hacking it is possible to gain a wide range of information on the company and its employee’s. It could also be used to find information on what the company is working on.

<https://www.csmonitor.com/Technology/2015/0731/Are-Internet-connected-devices-eavesdropping-on-our-conversations>

How to prevent this

The best solutions for this approach are the simple ones.

* Keep the Bluetooth capabilities off on the device so that it will not connect to any phones or devices.
* Also make sure all passwords associated with the device are changed regularly and are secure

Cons

The cons to this are that you will not be able to use the Bluetooth on the devices which add a level of ease. It will still be possible to gain access to the microphone using other hacking techniques. If the password is changed regularly it is hard to remember and sometimes not secure. This a low-cost solution because it is only keeping track of devices with microphones and being sure they have strong password and Bluetooth is off. That means it is minimal labor for employees who keep track of the IoT devices

Trust Between devices on the same network

When a device is automatically connected to others and trusted because it is on the same network. The network assumes the devices that are on it are secure and will allow connections automatically.

Why is this concerning

This is concerning because this is how viruses can spread through a system. It can infect one device and because devices tend to communicate with each other it spreads. When they connect and send data back and forth if the virus could attach to the data. Or send out a packet with the virus on it. With this method of spreading to devices it is possible to infect all of the devices in the office in a relatively short amount of time. From there it is also possible to spread on to the computers depending on the sophistication of the virus.

How to prevent this

The best way to prevent this,

* Implement a check point in your network it will assure the incoming requests are safe. When the devices send a request to connect to other gadgets on the network then it would go through a trusted network connection. That would assure that the device is not infected and not trying to infect other devices.

Cons

The cons of this is that you would have to buy the equipment to be able to check all requests for devices to connect to each other. Also you would have to be assured that when you implement it in your network it doesn’t not slow down the system. The cost of this is high not only because you have to purchase the device but because check points can slow down networks. It would take time and effort to make sure that it is not an issue.