VANDERBILT

Vanderbilt #ReadyForAnyChallenge

Cybersecurity: How to implement best practices

If you are looking to implement best practices to combat cyberattacks, here are five steps to consider.

1 Choosing the right equipment

One of the most obvious places to start is to choose equipment from reliable suppliers that have a knowledge and interest in cybersecurity and are focused on protecting your data. When your security system is designed from the ground up to protect against cyberattacks, naturally your organization will be in a much better place.

2 The weakest link

The most obvious low hanging fruit for hackers is to target people. Targeting people opens the door to the "weakest link" possibility that can uncover vulnerabilities such as lack of authentication and encryption, and weak password storage that can allow attackers to gain access to systems. Notably, most hacks come down to human error whereby weak passwords, or clicking on contaminated email attachments, will expose an organization's security. Hackers have also been known to target contractors and simply wait until they go on-site for scheduled maintenance with their infected laptops.

3 Regular updates

Cyberattacks must also be prepared for long after the product is released to market. As such, Vanderbilt creates regular firmware updates to keep a product in the field readily prepared to revoke the latest critical bugs that can flood the market, such as the recent Meltdown and Specter bugs.

4 Encryption

By encrypting anything before you send it to the cloud, it adds an extra cushion of control and power over that data. It not only provides an added defensive structure around a company's information, but it also adds peace of mind to the equation when relaying this data to the cloud.

5 Staying diligent

So how do we best protect against the darker side of an increasingly connected world? By being open and transparent in exposing and reporting vulnerabilities. The best way to avoid attacks is to keep systems up-to-date, change passwords regularly, provide employee training and be diligent in safeguarding facilities through firewalls and following best practices in network maintenance. Keeping up with security updates allows us to make the most of the new technologies available today and into the future.

What cyberattacks mean in an interconnected world

We probably take critical infrastructure for granted in our day-to-day living. We turn on a tap, flick a switch, or push a button and water, light, and heat are all readily available to us. However, as critical infrastructure are managed by computerized systems, this makes them vulnerable to cyberattack. As a direct consequence, this makes us as a society vulnerable too.

Imagine if a cyberattack took down the power supply to an entire city without warning? Chaos would ensue. Traffic lights, ATMs and cash registers, fuel pumps, and water pumps, amongst a long list of other things, would cease to operate. The scary thing is, the scenario of a cyberattack on critical infrastructure isn't far-fetched anymore.

What this means for physical security

The rapid gains that technology has made into everyday living has also changed how the security industry operates. In short, physical security has moved from being very simple inputs and outputs to being always-connected devices. This makes the industry very much part of the IoT world. Of course, this leads to the question - how does physical security protect itself from cyber vulnerabilities?

Kim Loy, Director of Technology & Communications at Vanderbilt

This ethos has changed how Vanderbilt think when designing and developing their security systems, in particular **SPC**.

What is SPC:

Vanderbilt's SPC is an intrusion detection platform that delivers a modern, powerful security system for your customers' needs. SPC protects businesses, properties, and assets. It is an intrusion detection system that offers versatile and comprehensive alarm management functionality. Through the use of cloud services, end-user apps, and a dedicated software suite, SPC is at the forefront of modern intrusion detection.

Built-in defenses

SPC has built-in protection mechanisms whereby if the system is attacked, it will go into protection mode. The system will remain operational, and it will still be able to communicate out, but it will start to shut down elements of itself to protect the system from the attack.

While no system is invincible, SPC has been designed so that should an attack penetrate, the system has multiple communication paths available as backup. Therefore, if one server is taken down the system can immediately switch to a backup server and then switch communication paths to bypass the attack and ensure messages still operate successfully.

John O'Donnell, Product Manager at Vanderbilt

Regular tests

Vulnerability testing is a must, and Vanderbilt always incorporates this into the development phase of products from day one onward. This thought process includes analysis of the type of cyberattacks that can potentially attack, breach, and disable a system. You then have the option to try and hack your product from within the organization or hire a third party professional group to attempt to do it for you.

The groundwork for many of the cloud's security worries is that organizations are ceding control of their data and depending on cloud service providers to preserve it for them. But cloud encryption delivers additional levels of defense, providing a useful antidote to this anxiety.

Ian Hanlon, Intrusion Specialist at Vanderbilt

Encryption

FlexC, Vanderbilt's communications protocol is a bespoke design that ensures everything is encrypted, all communications are monitored, and multiple types of attack are considered for defensive purposes to provide the best security possible. So, essentially what this means is, that this makes our cloud security extremely secure. The encryption used by FlexC communications between panels and the cloud is an AES 256-bit SSL encryption.

What is FlexC:

FlexC is a multipath, multi-redundant, highly encrypted communications protocol that allows secure monitoring and control of IP communication paths. FlexC was built from the ground up solely with cybersecurity in mind.

Where we're leading

With cybersecurity, you must act every week. It is not something where you can say, "we're safe, we're secure, let's forget about it." Every time you release a product or release an update, you must centralize your mindset on cybersecurity. Vanderbilt's fundamental way of approaching this issue is to stay in the mindset of assuming someone is currently trying to attack one of our systems.

> **So, when you look at the way our security solutions, like SPC Connect, are designed, you will see that they are built with that mentality in mind. People have a misconception that vulnerability announcements are a terrible thing. However, on the contrary, they can and should be viewed as a positive thing.**
>
> *Ronan Naughton, Product Manager at Vanderbilt*

Having an environment within the software industry of open disclosures only means that we can learn from mistakes, we can see how hackers are attempting to breach systems, and ultimately, it can help us stay ahead of the curve and one-step clear of hackers' latest intentions. Finally, when system vulnerabilities are reported, it means that vulnerability testing down the line will improve; the bar will continue to rise.

Facts

In 2016, the WannaCry ransomware attack infected over 300,000 computers around the world. Frighteningly, the virus was spread by something as low-tech as an email. Britain's National Health Services (NHS) was caught up in the attack. As a result, surgeries were canceled, staff reverted to pen and paper, and only emergency patients could be treated.

The most well-known example of a cyberattack on critical infrastructure was the attack on the Ukrainian power grid in December 2015 when 250,000 homes lost power as a result. Accessing the systems controlling the plant's circuit breakers did not require two-factor authentication, thus providing a security breach for the attackers to exploit with stolen credentials.

According to the Kaspersky Lab research, the percentage of industrial computers under attack grew from 17% in July 2016 to more than 24% in December 2016. The top three sources of infection were the internet, USBs, and email attachments.

A spear-phishing email was the technique used in an attack on a German steel mill in 2014. Here, the attackers gained access to the plant's network through an infected email attachment. The success of these non-complex methods would indicate low levels of awareness about how cyberattacks are carried out.

In a survey of nearly 600 utility, energy, and manufacturing organizations, only half of the companies had a dedicated IT security program.

Currently, a hacker waits an average of 146 days from having penetrated a system before they strike. Therefore, regular assessments give the opportunity to root out penetrations before they strike.

The danger of cybercriminals is genuine. Last year, a ring of hackers called the Carbanak gang was discovered by the Kaspersky Lab, where it was reported the ring had stolen over $1 billion from financial institutions around the globe.

There are already millions of smart home devices in the world, including smart alarms, locks, lighting, baby monitors, and thermostats and televisions. It is predicted that there will be more than 21 billion connected devices by 2020.

Hacks can also have dire economic impacts. For example, a possible hack that could trigger a blackout in North America is estimated to leave 93 million people without power and cost insurers anywhere from $21 billion to $71 billion in damages.

In a report by Cisco Cybersecurity in 2017, 35 percent of chief information security officers and security operations professionals said they see thousands of daily cyber threats, but only 44 percent are investigated.

The amount of data that IoT devices can create is colossus. A Federal Trade Commission report entitled "Internet of Things: Privacy & Security in a Connected World" found that less than 10,000 households can produce 150 million distinct data points daily.

About Vanderbilt

Vanderbilt is a global provider of security systems recognized for future-proof, high-performance, easy-to-use products. Vanderbilt strives for innovation in Software-as-a-Service solutions such as **ACT365** and **SPC Connect**, as well as product integration both within and outside of their portfolio offerings. Simply put, Vanderbilt is **#ReadyForAnyChallenge.** To learn more, please visit **vanderbiltindustries.com**, or follow us on **Twitter**, **Facebook**, and **LinkedIn**.

For more information, please contact:

Ross Wilks

Head of Communications

+44 2036 300 695

rosswilks@vanderbiltindustries.com