VANDERBILT

News

Examining the importance of vulnerability testing products

Thanks to technology, the world we live in today can be quite a simple one. For instance, home appliances such as TVs, heating systems, air conditioners, and lighting systems can now be controlled remotely using smart devices. We can also grocery shop, buy concert tickets, rent a movie, and order pizza via smartphones without having to leave the house.

The dark side of the coin in this fast-growing, technology-driven world, however, is **the threat of cyberattack**. 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.

With this in mind, vulnerability testing of your security solutions is a must. A security

vulnerability in a product is a pattern of conditions in the design of the system that is unable to prevent an attack resulting. This will result in perversions of the system such as mishandling, deleting, altering, or extracting data.

Methods of attack

With more connectivity over the internet, IP physical security systems can be vulnerable to attacks. Hacking an IP security system can take place through a variety of forms, some being quite simple. For example, in a brute-force attack, a hacker just "guesses" passwords. Given that most people choose easy-to-remember passwords, many can be deduced via simple algorithms.

Another standard method of attack is a Denial-of-Service. Here the offender attempts to overload the system by flooding the target with excessive demands and prevent legitimate requests from being carried out. This effectively makes it impossible to stop the attack by blocking a single source.

For instance, if a Denial-of-Service were to barrage and sink a Vanderbilt SPC panel successfully, the panel wouldn’t send any alarms. The Denial-of-Service would cause the panel to reset, rendering the alarm silent.

So, from this point-of-view, 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.

Standard practice

Essentially, this form of testing puts the product through its paces, and once weaknesses are exposed, they can be patched up, and the cycle of attack-and-defense can take place again until eventually, a watertight ship is in place and ready for market.

This is standard practice as even the Pentagon brought in hackers to help identify more than 100 security vulnerabilities in their systems. Reportedly, hackers that could locate security issues were awarded up to $15,000 each, with approximately 1,400 hackers taking part in the project.

While approaches like the Pentagon’s might seem dramatic, given the cash incentives they put up for grabs, when you consider how much people depend on online channels in today’s interconnected world, any security breach could lead to a devastating loss in

customer confidence and therefore revenue.

Testing is the critical discipline that helps identify where corrective measures need to be taken to rectify gaps in security. The more extensive an organization's security testing approaches are, the better are its chances of succeeding in an increasingly volatile technology landscape.

Where we're leading

Due to the practice of vulnerability testing, Vanderbilt has been able to change their thought process when approaching the design and development of security systems, **in particular, SPC**. This intruder detection system has been designed so that should an attack penetrate, such as Denial-of-Service, the system has multiple communication paths available as a backup.

Therefore, if one server is flooded and taken down, the system can immediately switch to a backup server and then change communication paths to bypass the attack and ensure messages still operate successfully. So, 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 further damage in the attack.

Unfortunately, vulnerability testing isn’t something that can just be tried and tested for in the development phase and then forgotten about. Cyberattacks must also be prepared for long after the product is released to market.

This is because, as technology continues to advance, so too do would-be hackers innovation in creating methods and means to tackle and take down a security system. 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.

Multiple lines of defense

A robust data security strategy must involve recognition of your product’s potential weaknesses. With IP physical security systems, it is now an endless game of cat and mouse in staying ahead of the latest threats and hacking innovations. Therefore, vulnerability testing is a valuable weapon in your overall defensive arsenal. As well, as vulnerability testing its systems, Vanderbilt has various other forms of obstacles and barriers to deter and deceive would-be hackers.

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.

FlexC, Vanderbilt's communications protocol, was built from the ground up solely with cybersecurity in mind. The 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 – basically, a 128-digit number that would need to be decoded to breach.

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.

What to keep in mind

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. To conclude, 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.

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 just means that vulnerability testing down the line will improve; the bar will continue to rise.

#readyforanychallenge