WEYTEC

Do it smart.

Whitepaper

BOLSTER CYBER SECURITY STRATEGIES

with WEYTEC Solutions

Cyber security or information technology security are techniques for protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Effective cyber security risk mitigation needs to address all potential vulnerabilities in an organization's IT landscape. In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements:

1. A system susceptibility or flaw,
2. Attacker access to the flaw, and
3. Attacker capability to exploit the flaw.[1]

Aside from firewalls, malware and virus protection, there are many more strategies that can be implemented to reduce vulnerability. WEYTEC solutions based upon the WEYTEC distributionPLATFORM minimize the risk of breaches of cyber security on two levels, by reducing attacker's access to susceptible systems and their capability to exploit these systems.

Managing critical processes

The ability to fully control and understand network traffic and transported digital content is the dream of every IT manager. Every hour thousands of new risk-bearing applications hit the internet. Keeping up with network security is a race against time, every day. Various companies have developed hardware and software to analyze, detect and report abnormalities or potential threats. All these technologies are useful and contribute to the risk mitigation process

One of the biggest threats is users who accidently or intentionally bypass IT security policies. The WEYTEC distributionPLATFORM (WDP) can be used to remove access for a user to any PC, server or device on the WDP instantly. Control of any device can be limited to the personnel responsible for handling any issues in the event of an incident.

Going phishing

Stolen or manipulated PCs

PCs stolen from an office create huge headaches for any organization. They can be used to gather intelligence about an organization's processes and cyber vulnerabilities. While the monetary loss is minor, exposed infor-

1 https://en.wikipedia.org/wiki/Vulnerability_(computing)

mation stored on hard drives can be disastrous. Every day, staff and third-party vendors, visitors and contractors get caught stealing computer equipment.[2] The ones that do not get caught possess critical information to breach the organization's security shield. According to one source, more than one million PCs are stolen every year in the US alone.3 The FBI estimates that 10% of all laptops purchased in the US will be stolen within the first year of ownership.[4]

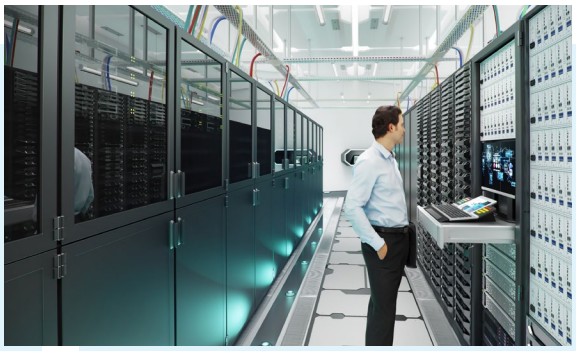
Malware Exploits

Stolen PCs reveal names of employees, their function in the organization, their contacts and their projects. Sophisticated hackers use tailored phishing emails that are very difficult to discern from real messages. Often, they are created with Information gathered from stolen hardware. At various security summits (e.g. DHS Security Summit 2016 and Homeland Security Summit 2017), multiple agencies reported attempted or completed attacks using highly sophisticated phishing scams that only could have been created with insider knowledge.

Physical access at the desk

Physical access to a PC encourages the use of the USB ports to charge cell-phones or exchange data from personal devices to social media or cloud services. Users can also easily copy data from the workstation to a portable hard drive. As seen with Stuxnet, the infection of a network can be achieved by the use of an infected USB flash drive with malware that meanwhile is so sophisticated (firmware modification) that it is undetectable even by the most advanced anti-virus software. This might be unintentional and without the user's knowledge. Cases are known where advanced users brought in bootable hard drives, bypassed the standard boot drive and copied data without a trace. If the PC is physically accessible, BIOS passwords do not help. Someone can pull the battery, reset the BIOS and copy data from the now unlocked PC. This will only be discovered if the admin specifically and regularly checks the conformity of passwords on all workstations. A logistical nightmare in larger organizations.

No PCS at the desk



Secured in a server room

All in all, there is a strong case for removing PCs from the workplace environment.

The WEYTEC distributionPLATFORM physically removes PCs from the user environment and sites them in secured, locked system rooms. Users have no physical access to computers. They cannot tamper with hard drives or upload malware through USB ports. And because the WEYTEC solution is strictly hardware based, physical access to transparent USB ports can be prohibited.

2 https://newsroom.intel.com/wp-content/uploads/sites/11/2016/01/The_Billion_Dollar_Lost_Laptop_Study.pdf
3 http://www.makeuseof.com/tag/stop-entire-desktop-pc-home-office-stolen/
4 http://www.thepicky.com/gadgets/how-many-laptops-are-stolen/#commentform

WDP versus Remote Access

With PCs distributed in offices, trading floors, and control rooms, software-based remote access for administrators has become the norm, at least in larger organizations. However, standard remote access by an administrator does not allow control of a PC at the BIOS level, and physical access to a PC at the desk can shut down any attempt by an administrator to prevent tampering. Also, software-based remote access is slower than WEYTEC's WDP technology.

The WEYTEC solution is strictly hardware-based. The WEYTEC distributionPLATFORM does not require any software installations on the systems. Also, it does not consume any of the PCs' computing resources. IT administrators can remotely control a PC even at the BIOS level completely independent of the operating system. Obviously, systems can be located in multiple on- or offsite data centers ensuring resilience in cases of infrastructure faults or site unavailability.

Incident Management

Incident management requires the immediate assistance or taking over control of a workstation as a help desk function or in response to a breach of security. With the WEYTEC distributionPLATFORM environment, incident management only takes seconds. Authorized employees can see a user desk via multicast from anywhere in the network and assist or take over immediately . The WDP cannot be disabled by the user or a malicious remote user. Specifically, a malicious user cannot use a local admin account to deactivate the WDP system administrator. That means that the WDP system administrator is still able to control the system in question. Authorized personnel can always assist, monitor all actions, immediately wrest control of a workstation away from a user and keep it. This feature significantly enhances cyber security by inhibiting an attacker's ability to exploit system vulnerability.

WEYTEC distributionPLATFORM

The WEYTEC distributionPLATFORM is designed to give users a better experience with complex (multi-workstation) IT environments and administrators a significant advantage in managing their IT.

Critical vulnerabilities can have a massive impact on the effectiveness of an organization and that directly impacts the bottom line. By using the WEYTEC distributionPLATFORM to control the PCs located in secure system rooms significantly mitigates crucial cyber security threats. The location of the PCs provides physical security, USB devices can still be connected to a PC but under a controlled process and IT staff can manage the PCs more easily than a physically distributed deployment.