Inside the Mind of a Cybercriminal

Common Steps to a Cyberattack and Six Steps to Prevent One

We're seeing a change in cybercrime and the way cyberattacks are being performed. A recent set of attacks against critical infrastructure entities expose a new approach to cybercrime and critical infrastructure hacks. Oil and gas pipeline operators, utilities and even some city and state governments; reveal the following new methods and motives.

Attackers were not out to steal data but were looking to disrupt services. Attackers used a new attack vector not previously seen. Instead of attacking primary targets directly, the attackers zeroed in on less secure vendors of those targets. We will be looking at how they did this along with how this can be prevented.

Step One – Reconnaissance

Before launching an attack, hackers first identify a vulnerable target and explore the best ways to exploit it. The initial target can be anyone in an organization. The attackers simply need a single point of entry to get started. Targeted phishing emails are common in this step, as an effective method of distributing malware.

The whole point of this phase is getting to know the target. The questions that hackers are answering at this stage are:

1. Who are the important people in the company?

   They discover this information by looking at the company web site or LinkedIn.

2. Who do they do business with?

   For this they may be able to use social engineering, by making a few "sales calls" to the company. Another way is good old-fashioned dumpster diving.

3. What public data is available about the company?

   Hackers collect IP address information and run scans to determine what hardware and software are being used. They also commonly check the ICAAN web registry database.

The more time hackers research and spend time gaining information about the people and systems at the company they're targeting, the more successful the hacking attempt will be.

Step Two - Weaponization

In this phase, the hacker uses the information they gathered in the previous phase to create what they need to get into the network. This could be creating believable Spear Phishing e-mails. These would look like e-mails employees of the targeted company could potentially receive from a known vendor or other business contact.

The next is step is creating Watering Holes, or fake web pages. These web pages will look identical to a vendor's web page or even a bank's web page. The sole purpose of this step is to capture your username and password, or to offer you a free download of a document or something else of interest. The final thing the attacker will do in this stage is to collect the tools that they plan to use once they gain access to the network so that they can successfully exploit any vulnerabilities they find.

Step Three - Delivery

Now the attack starts. Phishing e-mails are sent, Watering Hole web pages are posted to the Internet and the attacker waits for all the data they need to start rolling in. If the Phishing e-mail contains a weaponized attachment, then the attacker waits for someone to open the attachment and the subsequent malware to call home.

Step Four - Exploitation

Now the 'fun' begins for the hacker. As usernames and passwords arrive, the hacker tries them against web-based e-mail systems or VPN connections to the target company network. If malware-laced attachments were sent, then the attacker remotely accesses the infected computers. The attacker explores the network and gains a better idea of the traffic flow on the network, what systems are connected and how they can be exploited.

Step Five - Installation

In this phase the attacker makes sure they continue to have access to the network. They will install a persistent backdoor, create Admin accounts on the network, disable firewall rules and perhaps even activate Remote Desktop access on Servers and other systems on the network. The intent at this point is to make sure that the attacker can stay in the system for as long as they need to.

Step Six – Command and Control

Now they have access to the network, administrator accounts, and all the needed tools are in place. They now have unfettered access to the entire network. They can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees. At this point they are in control. They can lock you out of your entire network if they want to.

Step Seven – Achieve the End Goal

Now that they have total control, they can achieve their objectives or end goal. This could be stealing information on employees, customers, product designs, etc. or they can start interfering with the operations of the company. Remember, not all hackers are after monetizable data. Some hackers are out to just mess things up.

If you take online orders, they could shut down your order-taking system or delete orders from the system. They could even create orders and have them shipped to your customers. If you have an Industrial Control System and they gain access to it, they could shut down equipment, enter new set points, and disable alarms. Not all hackers want to steal your money, sell your information or post your incriminating e-mails on WikiLeaks. Some hackers just want to cause you pain.

So, what now?

What can you do to protect your network, your company, even your reputation? You need to prepare for an attack. Let's face it, sooner or later hackers WILL come for you, it's just a matter of when and how. Don't let yourself think that you don't have anything that they want. Trust us, you do.

When hackers hack, fight back – with these six steps

Step One – Enhance IT Security

Train your users and make them aware of what they can do to help protect the network. Tell them the evils that are out there, what to look for, and put a positive spin on it. Don't make the mistake of saying that 80% of people click on this evil link. Then the message is that the majority of people do it, and people tend to follow the majority. Instead say, "Good users don't click on links like this." Also, you need to know who your users are, when they normally log in and from where. Monitor the network for anomalies.

Step Two – Revisit Architecture

Look at your network from a different point of view - like a hacker would. If you were going to attack your network, what weak points would you look for? Be brutally honest with yourself. Don't be afraid to bring in a third-party penetration tester to test your network security.

When it comes to your network configuration; consider micro-segmentation of your network, with each department or group on their own subnet. This will make it more difficult for a hacker to move around your network, in the event they get past your firewall.

Step Three – Know What Is On Your Network

Map your networks. Discover all the devices connected to your network and know where the networks touch each other and the internet. Know the configuration of every router, switch, wireless access point, computer, printer, etc. that is connected to your network. Implement alerts when the configuration of one of those devices change for any reason.

Step Four – Create and Enforce Cybersecurity Policies and Procedures

If your company created cybersecurity policies and procedures two years ago and have not updated them since, they are most likely out of date. Review and update your cybersecurity policies and procedures, and then share with and explain them to your employees. If no one knows they exist or if they don't understand them, they will be impossible to enforce.

Step Five – Patch and Update

Microsoft and other vendors release security updates for a reason, and it is not just so they can send you an e-mail on Patch Tuesday. As soon as you become aware of a security related patch or update, make plans for when and how that patch will be implemented and how to mitigate the risk while you wait to install the patch.

Step Six – Detect Unknown Threats

This step echoes Steps One and Three. know your users and know your network. Look for anomalies, new devices, or new hosts on the network. If anything changes on your network due to your change management process and procedures, you should be aware of the change before it happens. Any change in a user's sign-on activities should be questioned. Don't be afraid of upsetting the users, they will be more upset if you get hacked.

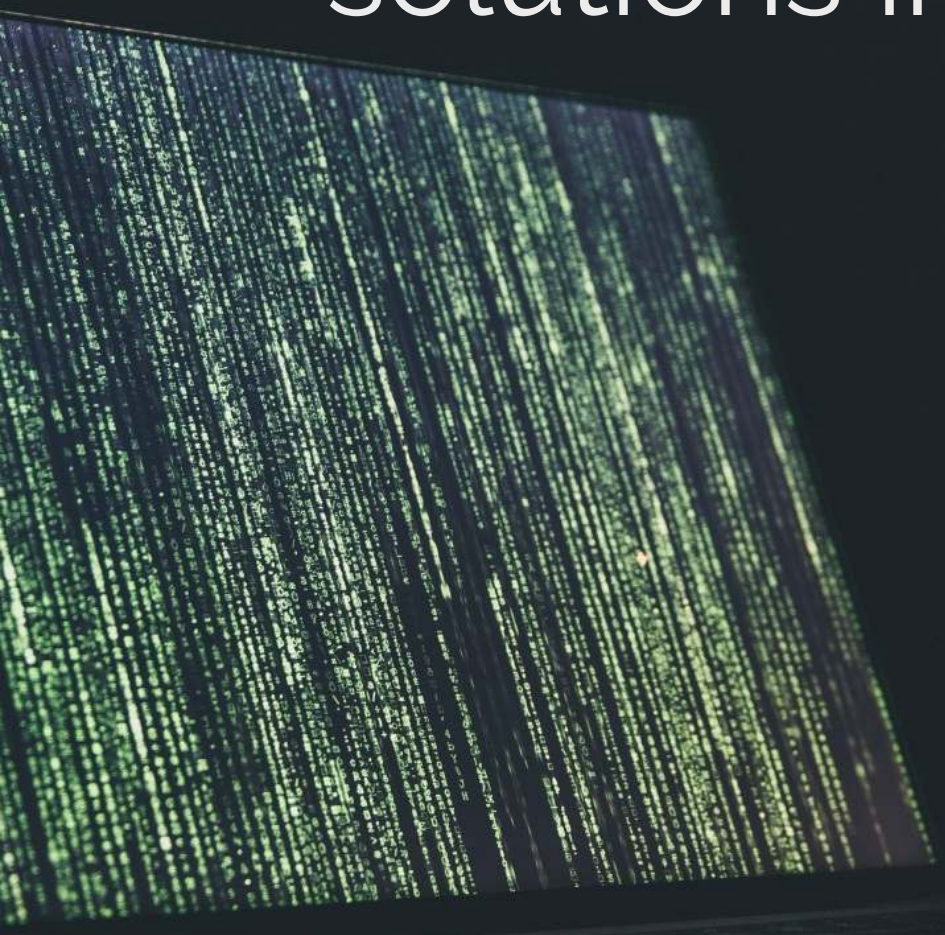
Employ A Proven Cybersecurity Partner

Velta Technology's cybersecurity team combines traditional IT best practices with a deep understanding of the sixteen critical infrastructure sectors and the employed operational technologies (OT). These sixteen critical infrastructure sector assets, systems, and networks; whether physical or virtual, are considered vital to the United States. Their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Our team of experts draw on extensive knowledge and experience in all relevant areas including risk management, operations, and human factors. This helps ensure all testing and the suggested mitigation measures are tailored to the specific needs of your industry as well as your unique business.

For a security, cyber risk, and vulnerability assessment at no cost to you; please contact us. Velta Technology's Senior Cybersecurity Systems Engineer Craig Reeds can set up a complimentary risk assessment for you and your organization. Schedule time here, or reach out to him at craig.reeds@veltatech.com or (314) 463-0470.

The most powerful cybersecurity solutions in the world.



Industrial Security for Point-to-Point Communication

An impenetrable barrier between defined endpoints within your existing network

Intelligence-grade, quantum-resistant security

Request A Cybersecurity Risk Assessment Report for Your Operational Technology (OT) Environment Here Today

Velta Technology