Your Business Through the Eyes of a Cybercriminal

A Guide to Where Your Business is Vulnerable and Steps to Lock it Down

R2 UNIFIED TECHNOLOGIES

SIMPLY BETTER

Table of Contents

eBook Sources

1. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
2. https://learn-umbrella.cisco.com/ebooks/trend-report-more-organizations-are-using-a-secure-internet-gateway-for-secure-access

Step 1: Reconnaissance

To the average cybercriminal, your business is built like a net; held together yet full of wholes.

Lockheed Martin has developed what it calls a "Cyber Kill Chain," a seven-step process that outlines how a well-resourced attacker would burrow into an organization. While this is a useful document, it's important to understand that criminals won't necessarily use it as a blueprint. Undisciplined or under-resourced criminals will skip around, moving directly from delivery to exploitation while skipping weaponization, for example. Many of them won't use malware at all.

The average business has more to worry about from these undisciplined attackers – there are more of them, and they still have a very good chance of breaking into your company using relatively simple tools.

Simple or sophisticated, the attackers are going to start at the same place: ***reconnaissance.***

The reconnaissance stage serves the purpose of identifying potential targets. Understanding if they have anything of value, and learning how easy or difficult it will be to attack them.

For example, they will:

- Go on social media – LinkedIn, Facebook, Twitter, etc. – and use the information there to build up an org chart of your company, including email addresses.
- They will find press releases about your organization. The information tells them who works for your company – plus it lets them know if you're growing.
- They will look at your website and assess it for vulnerabilities – are there any un-patched vulnerabilities?
- Lastly, they will try to map out your private network to perform the same kind of assessment. They'll try to understand the network security devices you're using to protect yourselves.

From this point, many attackers will find it easy to move directly into the exploitation phase.

Exploitation—*The Easy Way*

With reconnaissance, the attacker has discovered basic vulnerabilities your company may offer. Even though the kill chain has several extra steps, hackers can use some basic techniques to start stealing data right away.

Let's say that an attacker finds out the personal and business email addresses for your VP of Sales. The first thing they're going to do is check to see if those email addresses have been leaked in any previous data breaches. This happens relatively often. Attackers frequently dump stolen customer information on publicly available sites like Pastebin after they're done using it.

Next, they're going to see if the emails in that same breach have passwords associated with them. Again, this happens often. Some users keep using their old passwords because they don't know they have been breached. Others just don't care. A recent study by Google showed that 1.5 percent of users still use old passwords even after they've been known to have been breached.

Since users recycle passwords across different websites, the last step for the attacker is to take any associated passwords associated with the VP's email addresses and try them elsewhere. Since the target is the VP of Sales, they see if these logins work with Salesforce. If they're lucky, then the attack ends there – the passwords work, you have no two-factor authentication in place, and the attackers can just log into Salesforce with an admin account and steal the data that's in your CRM.

A lot of cyberattacks end this way. Attackers just have to do some basic research, get a little bit lucks, and then sign into a trove of information – basically without using any malware or interacting with their target in any way. It's not always that easy, thankfully, which means that it's time for another approach.

Let's say that the attacker isn't lucky and wasn't able to find login credentials by essentially Googling them. What else is left? Unfortunately, attackers still have a plethora of options. Most likely, they will try a phishing attempt involving malware or a basic social engineering tactics. These will usually involve email – over 90 percent of cyberattacks begin with spear phishing. In rarer occasions they will attempt to breach your website or network directly.

Over 90% of cyberattacks begin with spear phishing

Step 2: Weaponization

In the likely event that attackers go with an email-based attack, the attacker still has to flesh out a bit of a decision tree. For instance:

- Who do you target within the organization? Typically, attackers will go with a target that has enough authority to have access to something useful, but some scams such as BEC require targeting mid-level employees. (More on this in a second)
- They also need to understand if they're going to harvest a user's credentials – which means that they'd have to create a phishing site – or if they want to deploy malware.
- Lastly, if they choose to deploy malware, they need to choose what kind of malware to deploy. This has been an easier choice of late – Emotet is now in use in over 60 percent of phishing campaigns – but Emotet can have a variety of effects. Do they want to configure ransomware to drop a banking trojan or do they want to use ransomware?

These decisions, once again, will be made based on the results of the reconnaissance phase. The kind of security you bring to the table will determine whether they use malware and the kind of malware they will use. Your org chart will determine the target. You should use these considerations to harden your defenses accordingly.

Step 3: Delivery

This is the part where your attackers send their phishing email campaign, deliver their malware, or try to hack your network. Depending on what they planned in the step above, this step can unfold in very different ways.

According to Cisco, "Often, attackers are looking for ransom: 53% of cyberattacks resulted in damages of $500,000 or more."

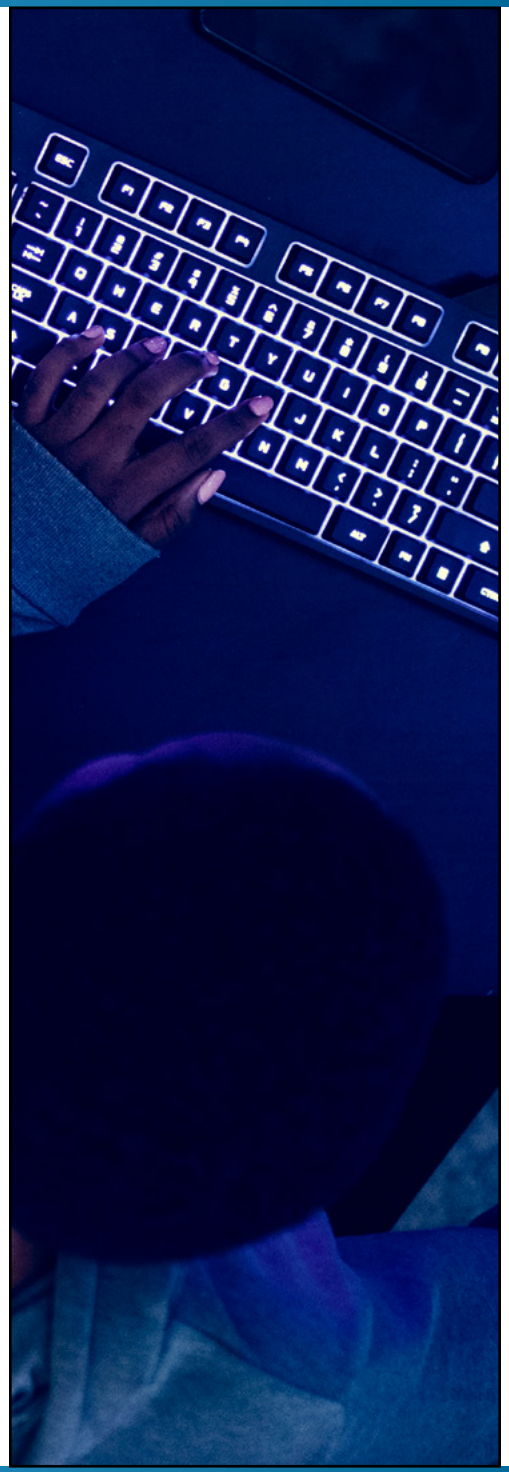
For example, they can choose the relatively easy way – one that involves neither malware nor phishing sites. Instead, attackers will choose a mid-level accounting employee and pretend to be their boss or an associated vendor. They'll send a fake invoice that looks exactly like the real thing, and the employee will usually pay the invoice without a second thought. This method, known as Business Email Compromise (BEC) scammed businesses out of $1.3 billion USD in 2018 alone.

Some forms of phishing don't use malware directly. Instead, they'll send an email pretending to be from some legitimate service such as Google, asking the user to log in. Instead of logging into Google,

however, your targeted employees will be handing their credentials over to an attacker. In other cases, this phishing site will also drop malware into the user's browser.

Business Email Compromise (BEC) scammed businesses out of $1.3 Billion USD in 2018 alone.

Finally, the attacker may try to send a viral payload. This will involve either a PDF or a word doc, probably made to look like it's coming from a boss or a colleague. Once your employee opens it, it will execute on their computer. Your endpoint protection software may not be able to stop it – malware such as Emotet is designed to be polymorphic, meaning that it changes its signature automatically to make itself invisible to most forms of antivirus.



Step 4: Grabbing Your Data & Getting Out

At this point, there's almost nothing to stop your attacker. If they've successfully dropped malware onto one of your endpoints, they have a window into your network. Attackers can perform detailed scans to find which of your servers have vulnerabilities. Assuming that they're relatively cautious, they can move laterally through your network to find a data store of valuable information. Depending on your protections, they can either ex-filtrate data slowly – via FTP, for example – or do something as brazen as simply emailing it to themselves.

Ransomware is expected to cost businesses $11.5 Billion in 2019 with the top three most damaging threats being Malicious crytomining, Ransomware, and phishing attacks.

It takes companies an average of 206 days to detect a cyberattack. Most hackers will be long gone before any alarm bells start to ring. Most won't even have used malware to conduct their breach, meaning that there will be little trace of their crimes. It is hard, if not impossible, to mitigate the effects of a cyberattack after it takes place.

How Should Companies Respond?

Despite all the buzz about security and staying prepared, malicious attackers are more audacious than ever. How can you address those vulnerabilities? *Together*, with a strong partner who has internal skills and experience to build a unified front against cyber crime and cybersecurity threats. The answer requires an integrated approach between unified systems and personnel.

While their is no single solution that will let your company detect and mitigate cyberattacks. You have to take a holistic approach, here's a few quick wins to test your network while you build added layers of protection into your policy:

1. **Training your employees to recognize and report phishing attempts when they occur**.
   People are the front-line defense for organizations, yet individual users are often cited as the weakest link in security. In a recent Cisco survey, only 51% of employees rated themselves as excellent at managing security via HR for on boarding and appropriate processes for transferring data on employee departures and terminations.
2. **Improve your email filters to recognize spoofed addresses and links to blacklisted sites.**
   No single cybersecurity technology can prevent phishing attacks. Instead, organizations must take a layered approach to reduce the number of attacks and lessen their impact when they do occur. Network security technologies that should be implemented include email and web security, malware protection, user behavior monitoring, and access control.
3. **Use embedded browser security that can recognize phishing sites.**
   Often called pharming sends users to a fraudulent website that appears to be legitimate. Attackers then infect either the user's computer or the website's DNS server and redirect the user to a fake site even if the correct URL is typed in. To combat this threat, we recommend upping your security and firewall protocols.
   Protect your employees and your data without disrutping daily productivity with secuirty appliances that will automatically block risky sites and test unknowne sites for vulnerabilities and unsafe access.
4. **Enforce multi-factor authentication.**
   Roaming users and devices are connecting directly to critical business resources with limited or no security. *Why?* Because centralized security policies are often no longer enforced, which increases the risk of a successful attack or compliance violation. Focus on multi-layed authentication of your network especially when you have a large contingency of remote workers or guests requesting access to your network or into your data.
5. **Conduct regular penetration tests.**
   When teams piece together security solutions from multiple vendors that aren't integrated, it often leads to alert overload – which doesn't help. Be sure to select a partner and determine what you're doing internally and what your partner is doing externally. Pen testing is a great way to ensure you're capturing vulnerabilities regardless of where or who is responsible.

Attackers are getting bolder and less discriminating. They're now targeting every kind of business, from every kind of business — small, medium, enterprise — in every location, from central headquarters to remote workers to branch offices. You can't stop them unless you know where they're coming from and what they want.

Right now, you may find that your company is vulnerable even to low-effort attacks that don't use malware. Your goal is to change that. With a combination of technology and internal policies, you can create a network and an environment that is resistant to all but the most skilled attackers.

"100's of apps are being used without IT knowledge in a typical organization."

Feeling a little uneasy about your business and your vulnerability to cyberattack?

Pro Tip: Don't do it Alone.

Let's Find Your Security Vulnerabilities

Schedule a security review with R2.

We'll have an old fashion conversation about everything from your current policies, preventative measures, and employee training practices and build some recommendations for ways to reinforce your envonirment physically and virtually.

If you're ready to take you business to the next level, it's time to partner with a team of technologist that are simply, *well,* better.

You Deserve Better.

We Need a Security Review

About R2 Unified Technologies

Headquartered in Boca Raton, Florida, R2 Unified Technologies is the team organizations turn to when they demand better technology services. From data, security, and cloud solutions to professional and fully managed services; we approach IT differently.

R2 is an extraordinary team of technologists with a genuine approach to delivering tailored solutions with precision execution. We will do right by you. With every integration, with every interaction, Always. Because with R2, your experience is *Simply Better.*

www.r2ut.com

R2 UNIFIED TECHNOLOGIES

SIMPLY BETTER

561.515.6800

980 N Federal Hwy #410
Boca Raton, FL 33432

www.r2ut.com