BATTEN DOWN THE HATCHES
Protecting Against the Inevitable

Jeff Horne,
Vice President of R&D and Chief Architect, Accuvant

James Robinson,
Director, Information Security, Accuvant
It was already a busy enough time. You have just been told you need to be part of a due diligence review of a company your organization is acquiring. There are meetings to be had, calls to be made and endless hours of work to be done. Then it hits you - the last time the company made an acquisition, it came under attack. The public relations plans indicate the deal will be announced publicly in two weeks, and panic sets in as you think about what's ahead.

But all is not lost, you realize, and now it's time to act. But what exactly should you do? After all, deciding to batten down the hatches is the easy part. How to do it correctly is where the challenge lies. Dealing with this type of situation requires understanding the threat and knowing how to apply that intelligence to your environment to bolster defenses. While many of us find ourselves in this situation, very few share information about how best to address it. In this paper, we will share some lessons learned from real-life situations that will help you develop a plan of action that minimizes your organization's attack surface and strengthens the walls around your most prized assets as a potential doomsday clock ticks down in the background. It may not be possible to do it all, but the more actions you can take to protect yourself, the more layers there will be between security and failure.
Getting the Ball Rolling

Rally the Troops

Two weeks is not a long time, so it is important to move quickly. First, rally the troops. Explain the situation, and get everyone involved. Begin organizing a game plan for communications - both internally to your employees and externally in the event of a breach. Employees need to understand that an attack could begin with an innocent sounding email about billing or a human resources announcement, or even a message about the merger itself. Spear phishing and whaling can be especially problematic with highly-motivated attackers, who often go the extra mile and conduct extensive reconnaissance via social networks and other means to find ways to tailor their messages and make them more attractive to their targets. With an attack on the horizon, it is worthwhile for organizations to conduct some focused security training to teach employees to be on guard. Picking up the phone to verify an email asking for a login or for the recipient to download an attachment could make the difference between a quiet night and a damaging breach.

While ideally this training would be given to everyone, it may be prudent given the time constraints to offer special training to certain employees. In its latest Internet Security Threat Report released in April, Symantec reported that in 2013 executive assistants and senior management were in the top three categories of jobs targeted in phishing attacks (aka whaling). That could be a good group of people with which to start. If you know the attackers are after intellectual property, consider adding anyone involved in research and development to the list. Turning humans into an intrusion prevention system is the first step in stopping any attack.

Once news of the threat has traveled up the chain of command, for IT it will be all hands on deck. Expect work to be disrupted. Expect databases and applications to go up and down due to emergency patching and the attack. And expect some of your staff to get burned out. Before you get started with the hard stuff, communicate with your employees about what is going on and how they may be affected.

Know Thy Enemy, Know Thyself

Understand the Nature of the Threat

When faced with this type of threat, your first move is to try to understand the threat itself. In the example above, the organization should consider what happened last time. In other cases however, there may be more specific information available about an impending attack.

In May, Anonymous threatened to launch the #OpPetrol campaign on June 20 to target international gas and oil companies. In the days leading up to the attack, security companies warned the industry to expect attacks that use the tactics observed in similar operations: distributed denial-of-service attacks, defacing of social media accounts and websites, data theft and attacking servers, and planting malware. The alerts also included information about tools the hacktivist collective has used, such as the LOIC (Low Orbit Ion Cannon), and advised organizations to monitor for unusual activity and attempts at social engineering.
Whether or not hackers with Anonymous successfully targeted those companies, every bit of intelligence about the hackers behind the threat is information that could be used to shore up defenses. One of the most important questions businesses should ask themselves is: what are the attackers after? Are they looking for specific data they can monetize? Are they looking for corporate intellectual property that could threaten a potential merger or embarrass the company?

If possible, involve the FBI so they can share general trends they know about and begin taking investigative steps against the attackers. The more that you know, the more effective your defensive strategy can be.

The above is true because different types of attackers have different motives and tactics. For example, sometimes hacktivists are not out for data. Instead, they want to make a public splash in the form of a massive distributed denial-of-service (DDoS) attack or by altering DNS records to point to a site of their choice. In addition, if it is a known threat group, there may be intelligence available about them. Several industries also have ISACs (Information Sharing and Analysis Centers) that attempt to facilitate the passing of threat intelligence between companies, such as the recently formed Retail Cyber Intelligence Sharing Center. These organizations, as well as commercial offerings from vendors, can serve as vital sources of information to help you build a better picture of the threat you are facing.

One caveat - do not treat an IP address the same as a DNA sample and jump to conclusions about who an attacker is based on that alone. In a world of proxies and compromised hosts, attribution is a tricky business. Making a false assumption could hamper your defense as you attempt to police traffic on your network. Not that IP addresses are useless - on the contrary, having a list of IP addresses with bad reputations can be extremely helpful in preventing attacks from known adversaries. Just don’t jump the gun and blacklist traffic from certain countries without proper evidence.

Take Stock of Your Environment

Defending against attacks also requires an understanding your own environment. A tactical risk assessment focusing on key areas is in order. Last year, the Independent Oracle Users Group (IOUG) released a survey of 322 data managers and professionals that contained some mixed news. According to the study, 70 percent of respondents said they had a high degree of awareness of databases in their organization that contained sensitive or regulated information. That is an increase from the roughly 50 percent with that awareness in 2010, but it is still 30 percent short of security nirvana. Yet having visibility into how many databases you have and which of them have production data or sensitive information is important for planning your defense.

Take a moment to make an inventory of your systems - authorized and unauthorized software and hardware - and identify any interfaces between external and internal systems. Mapping your network is important for understanding the connected devices in your environment. From there, try to get a baseline for normal activity in regards to data transfers in and out of your environment, as well as internal traffic to critical assets. Once a baseline for user and application traffic has been established, you will be better able to identify anything out of the ordinary.
Two fundamental issues that need to be understood are the location of your critical assets and what applications, users and machines can access them. This can be done using both automated tools and by interviewing application developers and database administrators, as they may know where sensitive data resides and what databases are critical to supporting vital business functions.

The goal here is to get a clear view of your network in order to allow you to apply the threat intelligence you have in a comprehensive way that will minimize your threat surface. But understanding the nature of the threat and the basics of your network is only the beginning.

Readying Your Defenses

Close Open Holes

Taking stock of your environment doesn’t mean just knowing where data is stored or what servers are publicly accessible over the Web. It also means knowing the patch levels of all your systems. While having software and hardware fully up-to-date would be wonderful, there are multiple reasons why patching can lag - patches needing to be tested, the financial impact of downtime, etc. A vulnerability scan can give you a clearer idea of your security posture. It is important for this scan to include both internal and external systems; focus threat scanning on the attack surface being targeted by the attackers. Determining what vulnerabilities to patch first can be done according to their severity - which bugs are most likely to be exploited, which ones can do the most damage if they are, and which, if any, are known to have exploits available in the wild. Another factor that should influence this discussion is what the most likely scenario is for the attacker. This comes back to the threat intelligence you have. Start with any information you have about how the adversary penetrated networks in previous attacks.

Guard the Gateway

There is a road to the safe that contains your crown jewels, and that road must be guarded. In place of traffic cops, you have firewalls, VPNs and network activity monitoring tools. The trick here is to apply the threat intelligence you have to make those roads safer. As mentioned above, organizations should have a sense of what normal network traffic levels and behavior is like. Using network and user heuristics, enterprises can detect anomalies, such as a spike in overall traffic or the number of malformed packets, or user accounts accessing applications they normally don’t. A jump in such activity can indicate an attack. For example, a spike in spoofed packets getting caught by your firewall’s egress filters as they leave the network could mean machines in your environment have been compromised and should be traced back to the source.

Protecting these roadways should also include closing any entry ramps which hackers could leverage, such as any TCP/IP ports that are not normally being used. Another area to consider is split tunneling, which has long been frowned upon by network security pros despite the speed advantage it can offer users looking to access resources on the Internet. While having split tunneling enabled can facilitate better performance, disabling it allows for security controls to be enforced on the gateway and prevents malware from hijacking a computer and accessing the corporate network via the VPN connection. If you are considering back-hauling your remote users’ web traffic, do a quick review of the capacity of your concentrator. It might make sense to look into cloud options if your services can be extended there.
Another important aspect of your defense of course is your firewall. Use this crisis as an opportunity to audit your firewall rules. This can be a very painful process, but keeping in mind that the organization is pressed for time due to the impending attack, there are some ways to simplify it. You can start by looking at rules that allow “any” service between two hosts. In addition, keep an eye for rules that specify “any” source or destination. While this may be perfectly justifiable, it could also be that the rule is old and was set at a time when there were fewer systems on the network, making the access broader than originally intended. Another bit of advice is to go after rules that overlap or cancel out other rules.

Just as important as auditing your existing rules however is designing new ones that can be used to thwart the upcoming attack. If possible, feed any threat intelligence about the situation into your firewall, intrusion detection and security incident event management systems to give your defenses an extra boost.

On the subject of access, organizations should pay particular attention to Remote Desktop (RDP) software. RDP is useful when an employee wants to legitimately login remotely to another machine, but that same functionality is useful to attackers as well. Software like TeamViewer should be monitored closely for the same reason. A sudden uptick in the use of these applications could indicate an attacker has made it onto the network. In addition, consider using firewalls to restrict access to remote desktop listening ports (the default is TCP 3389) and lock out users after a certain number of failed logins.

If your intelligence indicates it, your network security strategy should also take into account the prospect of denial-of-service attacks, which are a favorite tool of hacktivists. Fighting DDoS attacks is not particularly complicated. There are two primary strategies which can be applied. The first is to use existing on-site equipment to mitigate a DDoS attack. This can be done by configuration, tuning or additional services being added. The second is to use a cloud service that is always on or ready to step in if there is an attack. Keep in mind however that DDoS attacks are sometimes used as a means to distract personnel from more serious compromises. This kind of multi-vector attack was used against multiple banks in 2013 to mask fraudulent wire transfers that totaled into the millions. Don’t be fooled. Know your intel, and act accordingly.

**Defend Critical Assets**

Having mapped your network, it is now time to make sure the necessary security controls are in place to protect your most critical assets. This applies particularly to database activity monitoring tools, which your enterprise should already be using to keep tabs on user activity and block SQL injection attacks. In the event you do not use third-party tools for this purpose, the major database vendors - Oracle, SQL Server, etc. - have native activity monitoring features that you can turn on. If your most critical asset is a process system, focus on it. Know the uses, and have the maintainers question any anomalies. In addition, communicate with your vendor to let them know there are indications the solution is under attack and you might need help.

In the IOUG study previously mentioned, just 33 percent of the 322 participants said they monitored all their production databases for security issues such as unauthorized access or configuration changes on a regular, automated basis. Roughly 60 percent said they either were not capable or weren’t sure if they were capable of proving super users were abusing their privileges.
Not being able to keep track of super users leaves a door open for attackers to move laterally across your network. For that reason, organizations should audit user accounts to make sure that unused accounts or ones with excessive privileges are weeded out. This may involve some conversations with various business units to discuss their access levels to ensure they are in line with what is needed and no more. Remember, the ultimate goal of attackers in many situations is to steal data, a process that in many enterprises requires moving across multiple systems.

A final thought about databases - try to bring your database patching up-to-date. This can be a tall order due to the realities of testing and the business impact of downtime, but patching critical, remotely exploitable bugs is a key element in protecting your data.

It’s not just databases that need to be protected however; LDAP, Exchange and Active Directory servers make for juicy targets as well as attackers attempt to steal data. In the case of any of your centralized management servers, you should use network heuristics based off traffic shaping over the course of the week to look for any anomalies. If your Active Directory server inexplicably pushed an abnormally large amount of traffic to a server last night, it may be time for access analysis and a password reset. Along these same lines, careful attention should be paid to making sure appropriate firewall rules are employed to protect these servers as well.

There are other basic precautions to be considered when it comes to securing sensitive traffic on the network. For generic LDAP servers, make sure anonymous LDAP queries are not allowed, and use SASL or TLS/SSL to prevent passwords from being uncovered by an attacker’s prying eyes as he or she analyzes a data stream.

The end goal of course is to shrink the attack surface for these servers. As with databases, look to reduce the number of user accounts with unnecessarily high privileges and ensure that the principle of least privilege is in place.

Raise the Shields

Some individuals feel that antivirus is dead, but antivirus is far from dead and buried and can be the last line of defense when dealing with an attack. Still, antivirus companies realized years ago that signature-based detection was not enough. Their response was to add heuristic and behavioral detection for malware. Make sure this type of detection is turned on. This may result in some false positives, but that is a short-term inconvenience for a potentially long-term benefit of not being infected. You should also turn on detections focused on potentially unwanted applications and administrative tools. This will help catch tools commonly used by attackers that aren’t necessarily malware, such as PsExec or Windows Credentials Editor. Work with the vendor or partner to do a health check or talk with your MSP to get some help.

Beyond antivirus are data loss prevention solutions. DLP tools can be important pieces of a strategy for protecting enterprises by preventing hackers from exfiltrating data. In this case, the blocking features should be turned on and tuned to information you feel the attackers may likely be after. This includes obvious items such as critical intellectual property, but also data you may not have thought of - such as password hashes for your LDAP Directory or two-factor authentication seeds.

Monitoring Database Security

According to the 2013 Independent Oracle Users Group (IOUG) study only 33 percent monitor their production databases for security issues. Roughly 60 percent said they were not capable or weren’t sure if were capable of proving super users were abusing their privileges.
Passwords after all, are the keys to multiple doors. Getting users to choose strong passwords is often more easily said than done. Pen testers and hackers alike take advantage of this fact by using dictionary and brute force attacks. The most important users on the network – those with access to business-critical assets and applications – should be required to either change their passwords or make sure they are in line with best practices when you’re battening down the hatches.

For this reason, two-factor authentication for sensitive systems should be implemented - especially for individuals more likely to be targeted. Many of your organization’s critical assets now support multi-factor authentication, including Microsoft Exchange Server 2010 and Active Directory. In the same way, it can also be used to better secure sensitive applications such as Remote Desktop. Whenever a user is performing privileged activities, multi-factor authentication creates an extra layer of security between them and an attacker.

If possible, configure multiple group policy settings in Active Directory to allow admin groups to get more complex passwords. The goal is longer and stronger, with best practice being to use complex pass phrases with at least 16 characters. That will put a strong lock on the front door. But it may also be worth it to lay a trap for anyone who may break in. Consider setting up dummy accounts that have either no passwords or simple ones, but can’t log-in because the hours during which the account can be used is set to zero 24x7. If you see this account trying to authenticate, you know an attack is underway and it is time to act.

**Prepare for the Worst**

Unfortunately, even with the best preparation, things can and will go wrong. At that point, the company has to be ready with an incident response plan. The response plan should have a few key parts: processes for identifying the nature of the incident, containing it, remediating it and communicating information about it externally if needed. Familiarize yourself with your company’s incident response procedures and do a dry run if possible. If you need to design these procedures from scratch, they should:

1) Assign a chain of responsibility.

2) Establish policies for making key decisions, such as when to take a system offline or isolate it.

3) Have relationships with third-party remediation services and forensic analysts so they are ready to go when an incident occurs.

4) Take care of your people – set up hotels, decent food, even evaluate a 16x8 schedule where they are required to get some rest. Remember if people are going the extra mile so are their spouses, and it might help to give them a “thanks” for their overtime as well.

5) Rope in your legal and PR teams and ask them if they have any contacts or outside counsel that could help the company navigate the aftermath of a breach. In case the worst happens, your organization should also ensure it has a backup plan for critical pieces of infrastructure and file stores. Know what information will be key for you in the event your network is taken down, and be sure to test your capabilities by restoring a few files to a different location to be sure everything is working effectively.
That last point is critical. A solid backup and recovery plan can serve as a guide during the chaos that may ensue as staff members scramble to respond to an incident. A backup plan should define procedures for backing up baseline configurations so systems can be restored to their previous state. Organizations should move to backup the most recent system and user data in preparation for an incident. As part of the recovery plan, organizations should include a list of their critical systems and processes so that if there is an incident the business knows what systems to bring back online first. The plan should also outline how data or systems will be recovered, such as from backup tapes or by switching over to redundant systems.

Conclusion

Under most circumstances, telegraphing a punch in a fight is foolish. In cyberspace however, it is far from an anomaly. Some of your opponents want you to know you are about to be hit to underscore just how powerless you really are. But their telegraphing sacrifices some of their advantage, which gives you time to be proactive.

There are eight key steps you should take:

1. Organize the troops and educate the organization about the situation.
2. Gather as much intel about the attack and the attacker as possible.
3. Baseline your technical environment’s inventory.
4. Scan for vulnerabilities and prioritize your patching.
5. Map your network.
6. Shore up Web and remote access.
7. Deploy tactical defenses and traps.
8. Prep your organization’s incident response plan.

Use the forewarning as an opportunity to organize your troops and educate them on how they may be targeted and what the organizations needs from them. Take the time as well to get a clear view of your security posture. Focus on your most critical assets and perform vulnerability scans. Apply whatever threat intelligence you have to protect them.

Last but not least, get ready for the aftermath. Have a tested incident response plan ready to go, and have third-party experts ready to assist should an attack occur. You may not be able to prevent the attack, but you can raise the cost of doing business for the attacker, and forcing them to scale a higher digital wall may be the difference between a restful night and a sleepless one for your organization.
Accuvant, a Blackstone (NYSE: BX) portfolio company, is the leading provider of information security services and solutions serving enterprise-class organizations across North America. The company offers a full suite of service capabilities to help businesses, governments and educational institutions define their security strategies, identify and remediate threats and risks, select and deploy the right technology, and achieve operational readiness to protect their organizations from malicious attack. Founded in 2002, Accuvant has been named to the Inc. 500|5000 list of fastest growing companies for the last eight consecutive years. The company is headquartered in Denver, Colo., with offices across the United States and Canada. Further information is available at www.accuvant.com.

© 2014 Accuvant, Inc. All Rights Reserved. “Accuvant” is a registered trademark of Accuvant, Inc.