deepwatch

WHITEPAPER

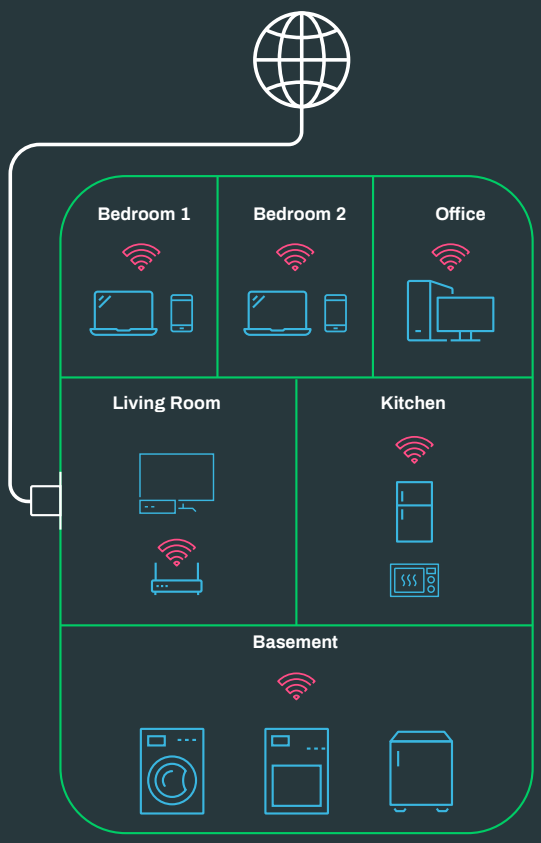
5 Best Practices for an Expanding Security Perimeter

www.deepwatch.com

Introduction

Virtual work environments and work from home have become the new normal for many commercial and government entities, at least since March 2020. Whether out of necessity, as in the case of continuing operations under COVID-19 shut down, or just the desire to change things around, the new conditions have expanded the boundaries for conducting business. With this new frontier, especially for those who have transitioned quickly, threats and potential attacks have also increased. Some of these risks now come from the most unprecedented places which would never be considered a potential problem or concern in a traditional office setting. Implementing best practices will not only help with managing the open security perimeter, but it can also minimize the risks and new vulnerabilities that come with the territory.

NETWORK DIAGRAM
Typical Home Setup



What is an expanded Open SecurityPerimeter?

In most cases, people think perimeter expasion means just going beyond our devices and moving beyond the office. They believe it refers to having a mobile workforce that may be working from coffee shops to homes and airplanes to Uber back seats.

An expanded perimeter means so much more. You really have to think about the impact of having your users going into a hostile network with some of these devices. You have to ponder whether network, mobile, or IoT devices are being used... have they even been patched recently or at all? Have the passwords been changed (or not) on laptops, desktops, or streaming devices? What kind of IoT devices are they running - vacuums, refrigerators, smart speakers? We have to remember we don't know what is on the networks that are now being used by employees. In essence, we are blind.

What major security policy mistake is being made by many organizations today?

Perhaps the biggest error business owners and executives are making today is emotional-based decisions, mostly due to a panic mode mentality. Decision-makers are putting a policy or action in place which can inevitably cause a break in the system or operations. These types of feelings based choices are reactions and should be avoided, as they will only set you back in the end.

State of Affairs – Then and Now

Pre-pandemic

For years, right up until February 2020 many organizations operated in brick and mortar structures, where there were plenty of layers of on-premise security to keep the compa

ny and the entire staff safe from outside intruders and bad actors. If a problem occurred with the system or a particular device, an IT or Help Desk member could take a five-minute stroll to a colleague's desk to troubleshoot and provide a quick fix.

Millions of employees throughout the world headed to offices daily to perform their duties, tasks, and responsibilities with little interruption. There may have been some hurricanes, Nor'easters, floods, and even tornadoes which caused isolated areas to temporarily shut down but nothing on the level of the deadly COVID-19 virus which brought businesses in the Nation, as well as many other countries to a grinding halt.

Some organizations, like Deepwatch, already had a large virtual workforce and were born out of the cloud. Others were either thinking about moving to the cloud or pondering about gradually transitioning to it. The recent pandemic caused organizations from Coast to Coast to make the move whether they were ready to or not.

Under prior circumstances, there were also all kinds of mechanisms in place to prevent intruders from accessing data, assets, systems, and employees right up to C-level executives who operated safely from the confines of their offices, behind firewalls, spam filters, and prevention systems.

Post-Pandemic

As COVID-19 continued to ravage the US and other countries, many organizations were forced to close their doors, at least temporarily or to re-think how they would be able to continue their operations under imposed shut-down decrees which prohibited all but essential workers to remain at home.

In order to prevent a greater economic catastrophe from occurring, a number of entities had their staff convert to a remote work from home arrangement.

Automation is one of those areas that gets more complex the deeper you go, but also offers greater potential value and return on time.

"According to Gallup Panel data, the percentage of employed adults saying they had worked FROM HOME SPECIFCALLY OUT OF concern about the coronavirus rose from 31% in midMarch to 49% a few days later, and to 59% the week after that. Remote work leveled of at 62% in mid-April.[1] "

1 "Reviewing Remote Work in the U.S. Under COVID-19." 22 May 2020, https://news.gallup.com/poll/311375/reviewing-remote-work-covid.aspx. Accessed 10 Jul. 2020.

Some made the jump in order to prevent an exodus of clients, a complete work stoppage or even to ward off the prospect of having to declare bankruptcy. Others did so to preserve their life's work after spending years and decades building up a business, brand, and reputation. In government, while not all employees were deemed essential, millions of citizens in America depended on public services, and these local, state, and federal entities had to devise a way of continuing to provide those offerings but through a virtual work setting.

In order to return to some type of normalcy, government and commercial organizations quickly made the jump to a virtual workforce and utilized the cloud to store information and data. Sometimes there was little or no thought to putting security measures in place or in determining how they would implement actions such as patches to resolve vulnerabilities with this new arrangement.

Even if the pandemic caused you to shift your operations quickly from an on-premise environment to a remote one, it is not too late to implement best practices now and apply the type of security measures which may prevent even greater devastation from impacting your organization, or worse a security incident.

Today's State of Affairs

With IoT devices that are being used for business transactions now, we are still talking about a typical home setup. Whether it is a setup for a day to day user or even a coffee shop, this is the environment you are now dealing with. It may be a setup in a bedroom used by three or four laptops, depending on how many people are in the house. It could be multiple streaming devices, Amazon echoes, Google android, and everything in-between.

Bad Actors search for points of entry they can exploit in order to execute their nefarious plans. In terms of IoT, someof those points of entry could include remote controlled washers and dryers, cooking ranges, and even refrigerators. In our world, everything is an app or should be able to integrate with other devices. This opens up the threat landscape significantly by way of a 3rd party which many don't have any guidance on how to secure or keep from talking to their devices. These aptly named smart devices could also be targeted areas of compromise, in addition to many others like smoke detectors, indoor/outdoor cameras, thermostats, speakers, and even vacuums.

When talking about a home setting, there are most likely some points of entry you never dreamed of posing a threat to your corporate assets.

In many states, children have spent months inside being homeschooled with a lot of extra time on their hands. They may have been able to get on to a workstation or laptop and caused adverse, unintended security consequences without the knowledge of the employee or IT and security staff.

What to Focus On?

Here are some of the areas which, just as before a crisis, deserve thought and action during a crisis.

Vulnerability Management Priorities: prior to march 2020, Organizations had to devise a plan and system whereby such Vulnerabilities needed to be identifed, classifed, prioritized And mitigated. Those vulnerabilities that existed on systems And new ones emerging, must still be dealt with under the new Environment. If you already have a patch management system In place, continue to use it and the same schedule. One thing to Consider with the remote workforce is that since the machines Are much harder to get to now, you will want to increase testing With the patching, taking into account more points of failure.

Cloud Based Strategies: If you already have a cloud strategy, you will need to continue to monitor, review and revise, especially in these times of constant change. If you had to transition to the cloud because of circumstances such as COVID-19, it is time to develop a cloud based strategy in order to determine how the cloud can beneft your organization while still keeping your applications and data secure.

Configuration and hardening: When we talk about confguration and hardening, this means several diferent things. The frst is performing just basic confguration and hardening on your golden images. This can be highly benefcial so that when you deploy a new system, there is not a need to install 200 updates. This helps greatly in keeping you ahead of the curve when deploying new systems.

Risk Acceptances or Exclusions Processes: Another item to hone in on is your process for risk acceptances or exclusions. You either have a formal risk acceptance process, or you have an informal one, where people are accepting the risk by just not doing anything on it. However, it would be appropriate for any entity to formalize their risk acceptance process. You will want to make sure it is getting reviewed and being used as a plan of action in order to give your IT team time to deploy what is needed. If it takes more than 30 days to deploy, that is FNE, because that is what the risk acceptance process is for.

Setting Home Security Expectations: You will need to set expectations that the company is not responsible for home network security. You may need to walk that line of providing advice, which is not the same as providing support. It may be benefcial to provide high level guidance on areas like patching network devices and changing default passwords. Creating a culture of security in the remote environment goes a long way.

5 Key Changes to Increase Security Posture Within Your Organization

1. Create a Disaster Recovery Program and Building an Asset Criticality List

Creating a Disaster Recovery Program is the first step in developing an Asset Criticality List. Every organization should have some type of Disaster Recovery Program although many do not know where to even begin.

If you don't not know who to talk with about the DR plan, you may want to begin with your business continuity group or your risk registry group. If your organization does not have such teams, it will be the IT infrastructure team who most likely has that tribal knowledge. These teams will know what the level one systems that if they go down, will be the first systems that need to be back online.

A business continuity strategy may already be in place to help maximize the efficacy of existing resources and locations, protect digital assets and investigate options and scenarios for extended workforce impacts. If so, check this plan to see if a disaster recovery program is already available.

Determine what systems have databases, web servers in particular, and build your asset criticality list from there. You will find yourself slowly building a disaster recovery program, or updating your current one. But most organizations already have these and it's just a matter of finding out who controls it.

One other trick is to talk to your business operations side and/or your accounting department and just ask them what computer systems would put the company out of business if they went down. They will have a pretty good idea of which ones are the most critical.

They will probably be glad that someone asked, as sometimes they feel like nobody seems to care. They will probably mention names of applications rather than names of computer systems, but you can take the information back to your IT team and tell them the systems that the business side of the house would define as most critical. They can tell you what they know about these assets, their operating system, and what dependencies they have. Your IT team can then go and incorporate the information and use it to ensure that the necessary items and systems needed are prioritized so you can still generate revenue. They can also make sure the dependencies are also on the list, such as an Active Directory and database systems. Those two are usually always necessary to make sure your critical systems are able to function under any circumstances.

2. Set Priorities Because If Everything is a Priority... Nothing is a Priority

While everything may seem to be important, there is a real hierarchy for prioritizing applications and systems. You really need to remain focused on business critical functions and make sure that the devices involved are getting the attention they need.

It is also important to note that there may be a priority change as well when circumstances change. Today, your VPN server is more critical than ever to business continuity. Things like VPN and web servers may be at the same level for criticality, whereas three months ago, that was not the case.

Therefore, if you had an asset criticality list, or you never created one, it is time to start preparing for a future event where your systems may go down and what that looks like from a continuity perspective. You should have a plan in place and prepare your organization in the event your company experiences such an occurrence. You have to discuss what it means from the functionality of the **systems, all the way down to the user level. This is mainly because with your finance team being at home or your CEO being at home, or anybody with PII information is a better target than the janitor**

5 KEY CHANGES TO INCREASE SECURITY POSTURE WITHIN YOUR ORGANIZATION

These types of issues are really what you want to start taking into consideration and determining whether tighter restrictions need to be placed around not just the functionality of the systems, but potentially around some of the users as well. You will have to think about the consequences to the organization if the information and data they possess were compromised.

Does this user need credentials? Do they need to log on to this application? What are the risks involved? What are the impacts of those risks? And then what can you do to mitigate them? What are those mitigation factors you're going to be able to put in place now to help. We have to remember what we had in place previously may no longer be valid because our users are working from home, and the ability to control what they are connecting to is no longer possible.

Take for example a vulnerability found in Citrix hardware devices which came out in late December 2019 followed by a patch in January 2020. What was discovered looking for the vulnerability in different networks was that it tended to be more internal with little external deployment. At that time, Citrix was likely used by a small subset of users. So its asset criticality was on the medium to low range, definitely not business critical.

The impact of the system was internal only and it was protected by a firewall. The mitigation factor was the firewall protection, as well, Citrix very quickly released a mitigation before the update came out to take care of most of the problem. It was intended to be an interim solution.

You may very well have looked at this and decided the steps you had already taken were good enough. We don't need to take these systems down to patch them. It's internal. It's protected by a firewall. The impact is low.

Now fast forward to three months later and you are in desperate need of a remote access solution. You need this immediately. You do not have time to order equipment or the budget to do so.
It is very tempting to take the Citrix system and repurpose it as a work from home solution. All of a sudden, asset criticality is at its highest. Your mitigation factor, the firewall, is not in place anymore. This application is external now and you do not have that level of protection anymore. The impact is extremely high. Your people can't work if this system goes down. What was a reasonably safe solution in January, is no longer a safe solution now.

Do not have an emotional, knee jerk reaction to this dilemma. Do the math. Does the math still work? Mostly likely it does not. Take a look at the situation. If you had a risk acceptance on this, make sure that you review it and make sure that the risk is still acceptable. If it is, continue to accept it. If it is not, contact your stakeholders and schedule the discussions to update.

3. Establish Hygiene for Your Home Network and Ensure Proper Security Training

Provide information to your employees about home network hygiene. You can do that without having to provide outright support. There is a very good chance your users are getting advice from somewhere, it might as well be from you.

Some of the information and advice they receive from elsewhere is good and some of it is terrible. There is advice in the technical press, but that's a technical press. When talking technical press computer advice, you may get someone who thinks they know better and will say they do not use antivirus and you should not use it either.

Sometimes they will get advice from social media and that is usually very questionable information. Again, you are going to find people who think they know more about security than the professionals. But Remember, you do have that knowledge and the respect of the people who work in your company. Use the position you have. You are giving trusted advice to your users.

It will counter what they are hearing about not having to update their phones, or that they don't need to update their home system, or that it's okay to run Windows XP systems so they continue to play their favorite game.

You will need to provide them with recommendations and explain the need to be keeping network connected devices up to date. You should provide them with feedback on best security practices and why they should not reuse passwords. Recommend the use of a two factor authentication system where they can, or even using a password management system. It is better to have 20 stored 16 character passwords than to use the same one over and over.

WINDOWS

- ✓ CIS Control 2.62 – Number of Previous Logons to Cache
- ✓ CIS Control 2.59 – Machine inactivity limit
- ✓ CIS Control 2.49 – Prevent users from installing printer drivers

BROWSER – FIREFOX

- ✓ CIS 2.2 – Automatic Software Updates
- ✓ CIS 8.4 – Block Reported Attack Sites
- ✓ CIS 4.2 & 4.3 – TLS max/min version

BROWSER – CHROME

- ✓ CIS1.3 – Allow remote users to interact with elevated windows in remote assis tance sessions
- ✓ CIS 2.16 – Set the time period for update notifications
- ✓ CIS 5.1 – Enable submissions of docu ments to Google Cloud Print

MAC OS X

- ✓ CIS 4.2 – 'Disable Screen Saver' setting in Hot Corners
- ✓ CIS 8.1 & 8.2 – Cloud Drove Document / Desktop Sync
- ✓ CIS 12.15 – Status of the 'root' account

4. Apply Confguration Guidelines and best practices to company owned devices

You should also take a good look at configuration guidelines or benchmarks, such as those talked about by the Center for Internet Security (CIS). There are a number of items which CIS can be helpful with if you are brave enough to dive into them. These benchmarks/configurations assist you in setting best practices for the applications, Operating Systems, devices, and more. These best practices in turn, allow your organization to have a better security posture by limiting the attack options on a users machine. For example, there are many different types of browsers available for download at any given moment. Depending on the browsers your orginizations allows or doesn't allow, you may want to implement CIS benchmarks for as many as you can, or at least the more popular options. By implementing these changes before a user has access to the machine, you can greatly reduce the risk of security incidents from these attack vectors. One very popular option that many organizations use today is the Hardened Gold Image. Which is a standard image used to implement user devices that has all of the configuration changes or benchmarks in place. This greatly reduces time and worry for the security team, since the changes and safeguards are in place before the user touches the device.

5. Don't Forget Your Third Party Applications

This is where your emphasis really needs to be on web browsers, Microsoft Office, browser plugins, Adobe products, and in some cases, your own in-house application. You may only support one third party browser, but you will have other third party browsers that are installed whether you're supporting them or not. If they are there, push updates to them. If they break, you are not responsible for supporting that browser, but you are responsible for the security of that device.

The likelihood of breaking, however, is very low. And it is better to ensure that those unsanctioned browsers are still getting those updates, especially since it will help in securing that device further, and possibly mitigating a vulnerability that would lead to a breach.

Conclusion

Create a Disaster Recovery Program and an Asset Criticality List before it is needed. When you are faced with extreme circumstances beyond your control such as the spread of COVID-19, which greatly impacts how we do business, you can rely on both the program and the list to get up and running with minimal disruption. In the event you were not able to develop either one, take a step back now and think about an action plan. Make sure you are looking at the situation without emotion and say to yourself, "What is going to be the impact to my organization if I do this or if I don't do that? Make sure you write everything down or at least retain notes of some sort not only about the proposed actions, but the thought process behind it, too.

Speak to your employees about security so you can guide and advise them. Also let the users know that such advice is not the same as actual support. Try to create the culture of security, so that your users are well informed about securing their home environments Continue to focus on vulnerability management priorities and other security measures which were important before the crisis and which are still vital now. While no one is sure how long COVID-19 will impact our economy and the way we do business, developing plans now to minimize your organization's risks will not only help your stability for today, but will go a long way in making sure you will be able to operate in the event another catastrophe arises as well.

What's Next?

Your business is only as strong as your security posture. Deepwatch Vulnerability Management Services serve as a baseline for us to collaborate to discover the critical assets, threats and vulnerabilities relevant to your organization. Deepwatch provides the people, process and technologies to fully or partially administer vulnerability management programs that fit your unique needs and requirements. To learn more go to https://www.Deepwatch.com/vulnerability-management/ or email us at sales@Deepwatch.com.

deepwatch

ABOUT DEEPWATCH

Deepwatch delivers data-driven managed security services whileextending customers' cybersecurity teams and proactively advancing their SecOps maturity. Powered by our innovative cloud-native platform, Deepwatch is trusted by leading global organizations to provide 24/7/365 managed security services.

CONTACT US

sales@Deepwatch.com
7800 E Union Ave, Suite 900 Denver, CO 80237
855.303.3033
www.Deepwatch.com