Things you wish you had done!

# THINGS TO HELP YOU IDENTIFY, PREVENT, DETECT, AND RESPOND TO CYBER THREATS!

**Ransomware and various other major cyber incidents are not fun to deal with, they hard everyone, from the end customer, your staff and ultimately your bottom line. We hate ransomware so we've put together a quick list of things to think about to help you prepare not only to prevent but also to respond so that hopefully your security posture holds strong but also if it does falter you can recover in a timely manner without any bitcoin payments being made!**

## DISCOVER ALL THE THINGS

I can't stress this enough; you MUST know what you are protecting (and from whom) if you have any change of defending successfully! Asset management is probably the most important cyber capability and organisations are struggling massively in this space (it's not sexy but it's so damn useful)

## BACKUP ALL THE THINGS (SECURELY)

Backup, again it doesn't sound all pew pew bang bang, but dammit get your business backed up! NOW… done it yet? What are you waiting for? Also make sure that backup is immutable so ensure it's NOT domain joined and send a read only copy somewhere (hell on tape if that works for you)

## AUDIT ALL THE PRIVILEGES

Honestly once again you see that work audit (it's not a bad thing, the NERD audit rocks compared to the accountant one 😁 ) . Get reviewing those admin rights, get reviewing those groups with high privileges both from an infrastructure and application point of view! No, you do NOT need to live in Enterprise Admins (or domain admins for that matter!)

## AUDIT THE FIREWALLS

This one is a Biggy! You would not believe the number of organisations that get owned because they exposed something mad like RDP or VNC to a high privileged asset to the internet!

## REVIEW LATERAL MOVEMENT POTENTIAL

It's great having SMB/RPC (TCP 445) open everywhere so that Jane in finance can connect to David in marketing PC but really, it's NOT! Go look at your data flow diagrams (hell just test data flows and write them down on a bit of paper if that helps you!) look at how an attacker that's inside your network could abuse legitimate functionality to move sidewards into your domain controllers and other assets! You have host-based firewalls for a reason, configure them good people! So in a windows world look at how RDP, SMB and WINRM are within your environment because if I was a criminal I'd be looking for wreak havoc and mayhem inside your network using those protocols (at least)

## PATCH PATCH PATCH

Honestly remember it's not just Windows updates, you need to keep your network secure as well, that includes patching your internet facing assets. Map your external assets and patch all the things (security appliances are a dumpster fire of RCEs so make sure someone can't just jump in and ruin your day). We still see blue keep exposed to the internet alongside a great many other OLD OLD OLD vulnerabilities, let alone when we look inside (Jesus I need another tea, get patching)

## PASSWORD AUDITS

If you use active directory this one isn't too hard to do, hell our friends at the NCSC even gave out a nice audit script which means you can do it with PowerShell (it uses DC replication so if you don't get an alert your defences/monitoring/alerts are somewhat lacking)

## DEPLOY MONITORING AND EDR

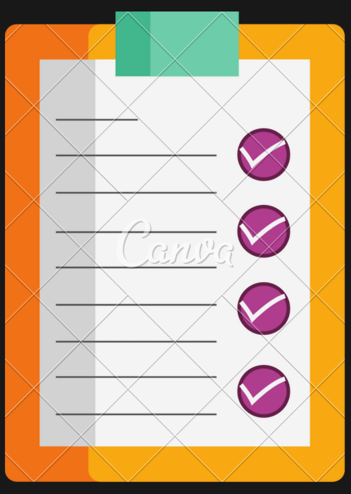
Honestly, you think your Norton home edition is going to help you protect against real cyber threats. Pah! Right if you have nothing deployed today at least deploy Sysmon (look at the SWIFT on SECURITY config or check our Dodge's config) but on top of that you want to have an EDR solution, don't think they are a silver bullet but damn they make life so much nicer!

Without logs you will find detecting and responding to be incredibly problematic. Logging, monitoring and alerting is a massive topic and can consume budget almost as fast as disk space but there's way to approach this even if you don't have the coffers to compete with Bezzos!

## HAVE AN ASSUME BREACH MINDSET

You think the world is all fluffy bunnies and rainbows? Well wake up people, the world is a nasty place, there are criminals out there looking to steal your data, to extort and hold your company to ransom. Please stop thinking "oh they just logged into a mailbox" or "I'm too small for someone to target" – trust me the criminals don't care. If they get one set of creds you can bet your bottom dollar, they are taking a copy of that mailbox faster than you can fill in a change request form! Be proactive with your security, it will pay dividends and you will be thanking me the day you watch the criminal's failure events in the audit logs!

## PLAN



Yes, this might sound bat sh*t crazy but you probably should have planned what to do when the sh*t hits the fan! This is so much more than the technical side; you need to involve the key stakeholders in the business and ensure you have a way to continually drill this process. Cyber incidents when they hit are very stressful so make sure you have planned to fail (we wrote a blog to help people think about common scenarios here: https://www.pwndefend.com/2020/08/16/have-you-planned-to-fail/

## There's no silver bullet and security aren't easy, but it doesn't need to be impossible

Hopefully this blog has given you some ideas of things you should be thinking about regarding cyber security (there's loads more such as MFA, decoys, allow lists etc. but this is a start!)

The criminals know this and will exploit this face! They do not care, and they don't stop, 24/7 365 days a year, so you need to make sure you, like the boy scouts, are prepared to identify, protect, detect, and respond to cyber incidents. Trust me, you don't want to wake up to a ransom note where you can't restore from backups! Be cyber safe and take care!

Source:

https://www.pwndefend.com/2020/10/27/things-you-wish-you-had-done-before-a-major-cyber-incident/