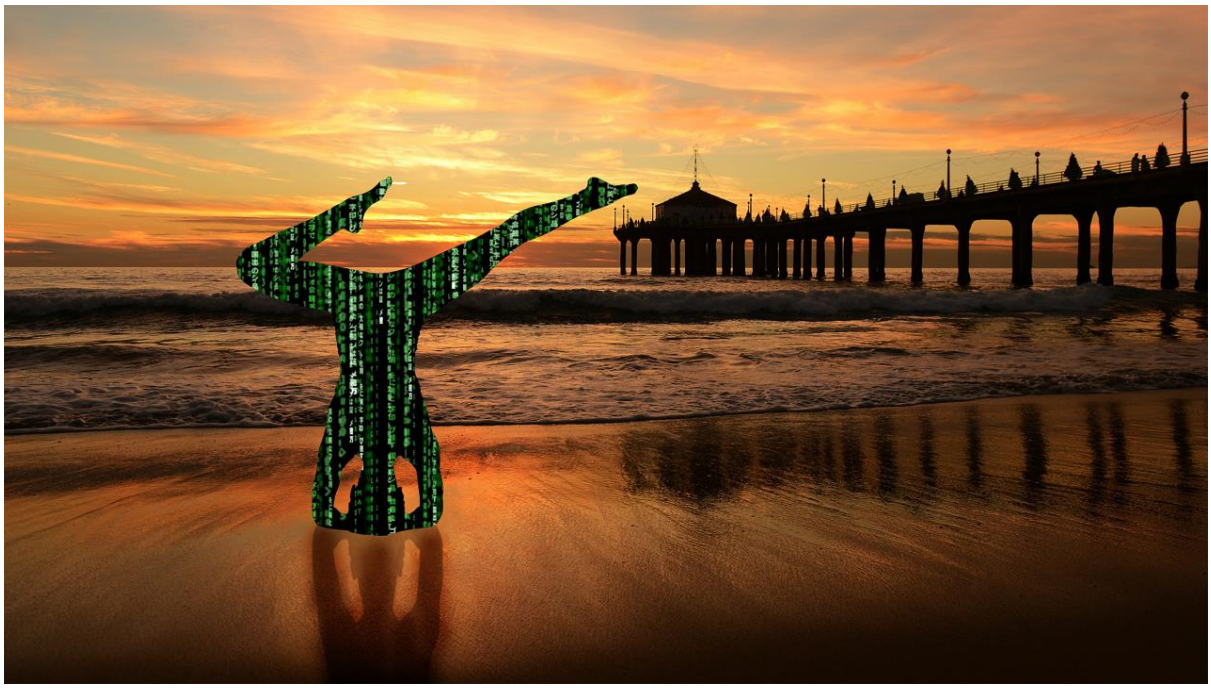
ADOPTING AN ENHANCED CYBER SECURITY POSTURE

Carl Ceillam, CEO, The Chain Limited

17th March 2022



Introduction

Over recent weeks we have seen a flurry of security advisories from organisations around the world warning us to be on high alert against cyberattack, and to 'adopt an enhanced security posture'. The precise nature and timing of the threat remains uncertain, although the latest intel suggests it is likely to be destructive data-wiping malware. There has been a consistent call to action from organisations such as the UK's NCSC and Jersey's cert.je to pay special attention to the following areas:

- patching
- access controls
- anti-malware defences
- logging and monitoring
- backups
- incident response
- internet footprint
- anti-phishing

Everything on the list is very important, but there's nothing new; these are all things that we are supposed to be on top of already. The threat of data loss, normally via ransomware, is also something we've been living with for a while. So where do we start when we have limited time and resources; how best should we respond, besides remaining 'alert'?

The short answer is that we need to think and act differently. We must shift our mind set from "trust and assume" to "understand and verify". Instead of thinking we have things covered, we must go a step further and confirm what is in place, and then check that it is working properly. To illustrate the point, consider these statements about anti-malware defences:

"We have anti-virus in place"

"We recently reviewed all of our anti-malware defence capabilities to validate that they offer adequate protection and are working as expected. We have identified a number of gaps which we are actively working to remediate."

The change in attitude needs to be swift, but the response can be pragmatic. We simply do not have time to identify and implement new technical security solutions, commission in-depth audits, or initiate a major programme of change. We need to work with and improve on what we have currently got.

In this article we will take a look at each of the general government advisories, and then highlight some of the steps you should be taking now to provide greater resilience and be more confident about your state of readiness for attack.

Patching

General advice is to make sure all software is kept up to date.

The first challenge is therefore to define 'all'. Take a fresh look at what systems and software you have on all computers, routers, switches, appliances, telephony, UPS, door entry systems, printers, the lot. And don't forget the smart TV in the boardroom. Check that there are effective procedures for identifying new security patches as they are released, and then applying them in an automated, controlled manner. Things like firmware may need to be handled manually, and you might not even know there is an update unless you subscribe to the vendor's mailing list. You should have quality checks in place to make sure that updates are applied successfully. Establish contingency arrangements for what to do if a critical security update fails to work, or legacy systems that don't receive updates.

Large organisations should already have this nailed but, but should still be double-checking that they have all devices in scope.

Access control

Strong passwords and MFA everywhere are still the common mantras here, plus we are reminded to tighten up on third party access. That's not new, what do we do differently today?

If you've had a security audit or penetration test you probably already know that your password policy is too short, but are hesitant to increase the minimum length for fear of a user backlash. Don't worry, the NCSC guidance works - three random words, with infrequent or no expiry; users soon get used to it. Push out educational communication on good password selection, then change the policy to 15 or more characters. The number of service desk tickets for password resets should actually go down.

With passwords taken care of, what about MFA? This is clearly a good thing but only if it is applied consistently and everywhere. MFA should be mandatory for all forms of remote

access, and for all privileged user access. In all likelihood you have conventional access paths protected, but other less well-known access methods exist that only require a username and password. Some common examples for Microsoft users:

- Exchange Web Services (and email services in general)
- Azure Portal
- PowerShell for Office 365
- ADFS
- Azure CLI

Find out what other access paths are open, and ensure they are all protected to an equivalent level. Wherever MFA is used, ensure that self-enrolment is disabled, and approval is required. This closes a potential loophole where attackers can hijack new or unused accounts.

Third party access - now is a really good time to challenge the external parties that have access to your systems. This may range from occasional contractors working on a project, through vendors providing support, to MSPs who control everything. Disable any accounts that are not regularly used, and only re-enable if and when they are needed.

Lastly, but by no means least, look at file permissions. The damage caused by a wiper or ransomware attack is proportional to the amount of data that users have access to. Review and tighten permissions to be as restrictive as possible.

Anti-malware defences

We are told to check that we have anti-virus installed and signatures are up to date. More specific advice might include the following:

- check the date of the last definition update for all devices
- investigate any devices that are falling behind
- use a test virus to check that AV is actually working and generating alerts. The EICAR test virus is a safe sample you can use
- enable anti-tamper protection so that users cannot disable AV

Verify that every type of system that supports AV is protected. It's not unusual to find some gaps. In addition to user PCs, these systems should be all be covered:

- public-facing web servers
- email gateways
- SharePoint Online
- content management systems
- file servers
- mobile devices (including personal ones)
- personal computers (including Macs) used when working from home

Backups

We are reminded to do backups, test them and make sure we have a recent offline backups, in case of a destructive data-wiper or ransomware attack.

That sounds simple enough, but this often an area where we confidently tell our auditors we have it covered, only to find that in a crisis recovery is slow and painful. Typical gotchas include:

- not all systems are covered, leading to data loss or downtime
- data is covered but configuration settings or access credentials are not
- cyclic dependencies, where recovery of system A requires system B to be running first, but system B needs system A first
- over-reliance on online backups which may lack sufficient capacity to deal with a high volume of data changes
- backup and DR tests lack depth and make assumptions about key infrastructure being in place

Checking backup coverage is relatively simple but requires a detailed review your estate, considering each device, system and application that may need to be recovered. Next, map out the dependencies for each backup solution in terms of hardware, software, network infrastructure, credentials, licence keys, people, and so on. Finally, revisit test procedures and walk them through from end to end, and challenge whether they provide confidence that recovery plans are robust.

Perform this review regularly.

Incident response plan

The official guidance is clear enough so there is not much to add:

- review and update the plan
- make sure it is clear on who the decision makers are
- communicate the plan so that it can still be accessed during all types of incident
- test it

On the last point the most effective test is a simulation exercise based on a real-world situation - malicious data loss would be a great choice. The simulation should involve senior management, not just IT, so that they get used to the drill, and learn to solve problems together.

Finally, if you haven't run a test for a while, this is definitely something to prioritise.

Internet footprint

This is about understanding what your internet presence is, both in terms of systems that could be targeted and also information that may facilitate an attack. Generally this is best assessed as part of a penetration test, but there are some basic checks that you can do yourself.

The first step is to identify your assets. Apart from obvious services like the corporate web site or remote access gateway, there are a range of other things to consider, some of which may not even belong to you:

- IP ranges allocated
- externally-facing systems
- DNS records
- SSL certificates issued and expiry dates

- domain name registration details, and contacts and expiry dates
- cloud platform tenancies
- employee details, including email addresses and phone numbers visible through social media

This is a good time to check that access to your domain registrar's portal is secured with MFA. If you have externally hosted DNS, then the same applies to your hosting provider. Both these moves will help prevent domain hijacking.

If your website is built using a popular CMS like WordPress then check who is managing it, and make sure they are keeping the plugins up to date.

If you have the capacity, run some vulnerability scans. Qualys have a simple to use but effective scanner which is free for small networks. Trial subscriptions to professional tools like tenable.io are available. Scans will help identify security misconfigurations.

Logging And Monitoring

The basic advice we are being given is to understand what logging is in place, and how long for, and then to actively monitor key logs. That's a good summary but there is a lot more to it. If you don't already have a log aggregator or SIEM in place, then put this list of actions on your to-do list:

- Windows event logs - enable Process Tracking, turn on auditing of login successes and failures. If log settings are default then it is likely the logs are too small and will be overwritten on a busy system in a matter of days; increase the log size to 150Mb or more; disk is cheap so don't hold back. Enable log archiving, so that logs are saved when full. These changes should be applied to all Windows devices, and will provide a basic but useful event history for investigation purposes.
- Firewalls - these devices can generate an excessive volume of log data, so it is normal to only enable logging for specific rules. When looking for signs of suspicious activity or intrusion, firewall logs can be one of the most useful information sources. Therefore it is important to make sure logging is at least enabled for the following connection types:
  - in-bound to all public-facing systems like webservers, VPNs, remote access gateways etc.
  - out-bound web browsing

  Talking of firewalls, take a good look at your firewall rules and check they are as restrictive as possible and have a clear business justification.
- VPN, Remote Access Gateways (e.g. Citrix, RDP/RDS, VMware Horizon etc.), and web proxies - check that the connection logs provide meaningful, actionable information. Can you tell who connected, from/to where, and when? Check that attempted and failed connections are logged too, not just successful ones.
- Public web servers - Web logs should be extensive and detailed, and retained for many months. Logs can get large so it is usually helpful to rotate them daily, so check this interval, and find out how far back the logs go. Alter these parameters to extend log history and detail level. As a minimum, every web server log should show the following data elements:
  - timestamp

- source IP address
- full request (HTTP method, URL, query parameters)
- referrer
- user agent
- result code (200,302,404 etc)
- response size

If your website is an application then it should have its own logs too. Check with the developers what information is captured. You should have audit trails enabled for authentication events, functions executed and data accessed. It should be possible to correlate the audit trail with the web server log by timestamp and IP address.

- Network devices, appliances and Unix-based systems - most should have some form of syslog logging already turned on. Check the log configuration, retention settings and ensure the logs are working.

That covers basic information capture. Unless you already have some means of collating and filtering logs for actionable data, then your immediate options for active log monitoring are probably limited to that. Instead, concentrate on maximising log value:

- make sure you can access and interpret each type of log
- scan through events to get a feel for what 'normal' looks like
- regularly check that events are still being recorded as expected
- ensure the logs are being retained for long enough (i.e. several months or more)

Another important aspect of monitoring is alerting. Some systems may have the facility to notify you immediately of critical events. For example, the disk is full or failing, a connection or signal has been lost, a system is unreachable etc. These are not necessarily security events, but help ensure the overall health of the monitoring environment. Turn these features on if you haven't already.

Anti-Phishing

We will assume everyone has had the training, emails are scanned for spam/phish/malware, and employees know how to deal with phish and to report them. What else should you be doing when the threat is heightened?

Web filtering. Blocking access to untrustworthy websites is by far the most effective way of neutralising phishing threats; if a sleepy employee falls for a scam email and clicks a link, nothing will happen if they can't access a fake login page or download malware. Action list:

- check your web filter categories are as strict as possible
- under no circumstances allow 'uncategorised' sites (now or ever again).
- block file sharing, webmail, peer to peer, upload/download, known malicious, scams, phishing, hacking, fraud weapons, hate and anything else that isn't work-related. Finally, if you haven't done so already, block social media (we're here to work, right?)
- blocks should be hard not soft, i.e. don't warn users of a dangerous then allow them to click through
- if you have issues with genuine legitimate sites that are blocked, submit them for recategorization.

- finally, check web filtering is actually working. Try and visit sites that ought to be blocked. Then review the logs to make sure the activity was recorded.

Conclusion

Switching your security posture from 'normal' to 'enhanced' is a tactical manoeuvre; it is not a call for new IT projects or a reason to invest in new systems. There is still plenty to do but the objectives can be summarised as follows:

- understand your current position
- work to improve what you already have
- keep a close eye on the things that matter

First published on LinkedIn on 11th March 2022.

Reference links

The Chain Limited https://chainci.com

National Cyber Security Centre https://www.ncsc.gov.uk

Jersey Cyber Security Centre https://cert.je

EICAR test virus https://www.eicar.org

Qualys scanner https://www.qualys.com/apps/vulnerability-management

Tenable scanner https://www.tenable.com/products/tenable-io