CYBERSECURITY PREDICTIONS & RECOMMENDATIONS FOR 2020

1 RANSOMWARE

Ransomware will continue to be a major issue for organisations.

Some predict this onslaught will fade out but this isn't realistic. The reoccurring revenue model is too rewarding for malicious actors and current protections **have not stopped these threats.**

RECOMMENDATIONS TO MANAGE THIS THREAT

Email Filtering & Click Protection

Adopt a strong email filtering system like Mimecast to help reduce the amount of malicious emails. Then, click protection will protect you if they make it through your first like of defence.

RECOMMENDATIONS TO MANAGE THIS THREAT

Enterprise-Grade Endpoint Protection

Implement enterprise-grade endpoint protection with the ability to detect and stop ransomware incidents in their tracks.

RECOMMENDATIONS TO MANAGE THIS THREAT

User Awareness Training

Humans are the most commonly targeted and the most vulnerable part of your systems. You need to give them the tools to identify threats and react accordingly. You could do online video training with short training packages sent each month, or onsite, customised training.

2 EXTORTION & SEXTORTION

Extortion and sextortion threat phishing emails are nothing new but are getting more aggressive in their approach, with recent examples like bomb threats and kidnapping. We feel this will pick up the pace with minimal change in the methods used.

RECOMMENDATIONS TO MANAGE THIS THREAT

User Awareness Training

Like ransomware, **training is key** to managing your threat level. Staff need to be taught about the problem and shown how to respond in the situation. This is because there are no malicious software or links, so staff need to know the process when they receive an email like this.

RECOMMENDATIONS TO MANAGE THIS THREAT

Email Filtering

Better email filtering will help to control the influx of these types of emails, which will reduce your risk.

3 PRICING REDUCTION

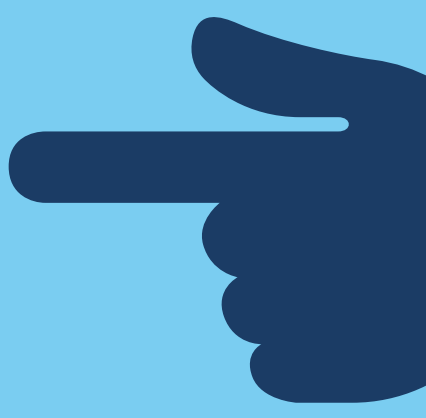
With the influx of security protection platforms and vendors, it is likely that existing vendors will be forced to reduce their pricing - great news for our clients! This will help us offer more advanced protection services moving forward.

Our **Davichi Assure** package provides you with the platforms and we manage them for you. This takes the stress out of it and allows you to take advantage of the best security measures available.

ATTRIBUTION: PUBLIC SHAMING OF APT'S

4

State-sponsored hacking groups known as APT's have become increasingly active in 2019; a preferred method of attack on other countries instead of physical wars. Davichi predicts this trend has not yet reached its peak and will only grow throughout 2020.



RECOMMENDATIONS TO MANAGE THIS THREAT - A MULTI-PRONGED APPROACH

Get the Basics Right

In addition to all of the above, you need to get the basics right. Update your systems, harden platforms and reduce the attack surface. If you don't need something to be available externally, then don't have it there.

RECOMMENDATIONS TO MANAGE THIS THREAT

Verify Your Cyber Insurance Coverage

You might have Cyber Insurance, but many policies **don't cover an act of war** which means no insurance payout.

Also many policies will deny your claim if you don't try to protect your systems, so you have to do your part in ensuring your systems are as secure as they can be.

5

ZERO TRUST SYSTEMS: A MINIMUM REQUIREMENT

Zero trust systems work on the least privilege, meaning that everything is treated as suspicious except what has been explicitly whitelisted or excluded.

Lock down data flow, control access at every point and take back control of your systems.

6

HARDWARE ATTACKS

Our improved ability to slow down attacks against our systems means malicious actors are also looking to bypass current protections and take advantage of our **hardware vulnerabilities.**

This means malicious actors can maintain a foothold on systems and continue to stay connected even after a reboot.

RECOMMENDATIONS TO MANAGE THIS THREAT

Stay Current

Keep up with announcements from your hardware vendors and make yourself aware of any known threats to any of your equipment.

Update Firmware and Sofware

Continue to update firmware and software for all of your hardware to ensure all security patches are applied.

GROWING COMPLIANCE REQUIRMENTS

The flow-on effect for the GDPR in Europe has had a ripple effect, with many organisations around the world finding it simpler to have one management standard across all of their locations.

Australian businesses will need to adhere to these expectations to work with larger organisations. Companies will want to become compliant with frameworks like ISO27001 without a mandated requirement to do so.

7

GROWING DIVERSITY IN CYBERSECURITY

Cybersecurity as an industry is still reasonably young and it lacks the diversity it needs to take back control from malicious actors.

Diversity in this case refers to more than just gender; we feel that diversity in culture, career background, skill set etc. is essential. We need to open ourselves up to the idea that the solution we are looking for might come from somewhere we least expect it. This diversity could allow us to get the upper hand in the cyberwar we are constantly battling.

WANT TO CHAT?

Email
Sales: sales@davichi.com.au
Support: support@davichi.com.au

Phone
+61(07) 3124 6059

Davichi