VENARI SECURITY

Whitepaper

Real Situational Awareness Is More Vital Than Ever Before

Paddy McGuinness

Former UK Deputy National Security Advisor, for Intelligence, Security and Resilience

Real Situational Awareness

I don't think there has been a day in the last few years where I haven't been helping a client somewhere with some form of cyber event. Ransomware has become ever more prevalent in 2020/21 but good old data theft, financial credential harvesting and insiders, malicious or otherwise, are still around. The most frequent organisational vulnerability that I find is complacency. This isn't about the scale of the risk - most CEOs recognise cyber/data/technology events as hard to price and deserving of effort and spend - but about the extent of situational awareness. Too often business leaders significantly overestimate what they know about their networks and external environment and underestimate the uncertainty they must learn to manage.

The composite picture which is given to Boards and Audit Committees in nicely tabulated coloured charts of internal monitoring, pen and phishing tests, dark web and scraped data analysis, threat intelligence from external providers and war stories from companies who have been afflicted by incidents creates a false impression of knowledge. In my business practice most companies do not communicate about an event unless they absolutely have to and when they must, perhaps for regulatory reasons, they are terse. The technical detail of what happened is rarely shared even internally. Forensic and remediation companies tell you about known exploits and malware which are a lag not lead indicator. Monitoring on your own networks inevitably has blind spots. At a rough reckoning 30-50% of what you would ideally know from all sources is not available to you. Perhaps that accounts for the extended "dwell time" of intruder presence in networks that we see in so many cyber events.

This uncertainty has previously been managed through a risk model but as a senior FTSE100 CISO friend of mine commented recently he feared he was a 2018 CISO operating on a balance of probability model which was inadequate in the face of the recklessness and aggression of the ransom takers of 2021 and the loss of controls caused by network change in the Covid19 Pandemic. Knowing as much as you can about what is happening on your network, keeping the length of that hostile presence to a minimum and having assurance once you restart previously affected parts of your network or reconfigured servers can be the difference between success and failure for a business - and a technology leader.

"Monitoring on your own networks inevitably has blind spots."

"The best of them [criminal actors] do not just bank on encrypted traffic escaping analysis, they disguise command and control traffic."

The recent Colonial Pipeline ransomware incident brings this to life. The operators did not know something anomalous was happening on their networks until it caused real world effect. The intruders had time to get organised. This contrasts markedly with an Operational Technology ransomware incident I helped with recently where the intrusion was detected within 5 days (which included a weekend) and though there was still some business disruption as the intrusion was cleaned out, it didn't knock the company over or have real world effect on the customer, the share price or the make-up of the leadership.

Encryption is increasingly seen as a panacea. One puzzled finance sector CIO tells me that their Board has insisted it be applied throughout their company networks. The Board thinks it will give assurance. The CIO knows that it renders many of their established means of detection and counter measures ineffective. And, of course, that it is actor agnostic. Many of the most aggressive criminal actors use TLS encryption to hide aspects of intrusion, egress and lateral movement in target networks amongst the other, perhaps too trusted and insufficiently monitored, encrypted traffic.

The best of them [criminal actors] do not just bank on encrypted traffic escaping analysis, they disguise command and control traffic as a legitimate encrypted data flow - Dropbox or cloud storage traffic. This is no longer cutting edge from the intruder. The defender needs to be as well equipped. Mainstream security providers highlight the issue and the too rare occasions when they have success. Greater certainty about what is happening on encrypted traffic flows is vital. This is where real situational awareness is required...

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.
16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.