SUPPORTING PUBLIC SECTOR ORGANISATIONS IN THE CURRENT THREAT LANDSCAPE

Paul Burrows
CEO, Kryptokloud

The UK government has made a huge effort to support the SME landscape by awarding more contracts to smaller firms. In 2017 it announced £3bn of IT investment over four years through the Technology Services 2 Framework, with SMEs expected to make up more than 60% of suppliers.

Such investments alert attackers who, in most instances, are after easy financial gains. Although they do not care whether a company is public or private, they see public sector targets as having a soft underbelly. Paul Burrows, CEO of Kryptokloud, an F-Secure Platinum Partner in the UK, believes this perception is correct: "We think that public sector organisations are at 70% greater risk than private organisations," says Paul, and there are a few reasons for this:

- Firstly, and perhaps most importantly, private sector organisations know better what they need to do to protect their business and can usually find available budget and plan accordingly. It has been muted many times that the public sector "knows the cost of everything and the value of nothing", but unfortunately, this has some resonance here. Things are slowly improving but getting budget for cyber security and planning for it are still seen as being too complicated.

- Secondly, there are now state-sponsored ransomware groups that have been tasked with undertaking recon ops to specifically target public sector organisations. We have seen this in several public sector industry segments, most notably further education - where there has been a recent dramatic increase in cyber-attacks against UK Colleges, Universities and in the sector as a whole.

- Thirdly, many public sector organisations will be focused on making their digital experience as easily accessible to the public as possible, which has the drawback of making them more vulnerable to attack – it is always a balance to ensure the enhanced "end user experience" is also well controlled and secure.

- Finally, the public sector struggles to attract the talent (internally) in terms of security professionals. This one is again linked to budget as well, but also to business priorities. Maybe they hire one IT Architect, who is also multi-tasked as a Security and or Network Architect and they will (unfairly) expect them to know and implement everything alone, which is simply not realistic.

KryptoKloud | F-Secure

LESSONS FROM LINCOLN COLLEGE

In mid-November 2020, KryptoKloud (Paul himself) received a call from Lincoln College at approximately 2am. The college had reason to believe they were being cyber attacked.

KryptoKloud's Incident Response (IR) team met with the college within hours and began the process of immediately assisting in containing the attack. This case is instructive because although the college's IT staff did many things right, there were processes missing and things they could improve upon.

Like most organisations, Lincoln College did not have a robust and tested incident response plan in place. This made it difficult for them to quickly action containment measures applicable to specific processes and technology. However, the college made the right call by contacting KryptoKloud immediately and listening to and acting on the IR team's advice throughout the entire process to the letter.

To their credit, the Senior Management including the IT Leadership and Staff at Lincoln College, adhered to a well-defined management structure, which allowed them to make decisions fast. However, and as is the case with most incidents, a response plan would have ensured a near automatic release of the first steps of containment, even before contacting an IR provider.

After the containment and investigation phases of the incident response activity, KryptoKloud were able to get Lincoln College back to "Business as Usual" within 13 days of the initial call. However, Lincoln College still had a further 21 days of grueling remedial work with their internal IT team. Having led the Incident Response – KryptoKloud ensured that all 3rd Party alignments and cooperation with outside agencies such as insurance bodies, ICO, Police and National Cyber Crime Agencies were fully informed, and all breach reporting requirements were carried out. This ensured final insurance payments were secured. It is also interesting to note here that cyber insurance providers will only pay for repairing the impact of a breach and not for improvements to your defense(s) or any system hardening measures.

In addition to the containment, investigation and response phases of the recovery, KryptoKloud assisted the college with the reporting and other compliance aspects of the breach, as well as assisting in public communications. What an organisation says and does in the wake of a breach are indeed critical to its future reputation.

AREAS FOR IMPROVEMENT

Lincoln College were very quick to recognise the shortcomings of their sector's approach to cyber security. All education facilities must consider new ways to tackle the common issues highlighted above.

For example, because universities and colleges are generally not able to attract or retain the kind of security talent found in the private sector, innovative apprentice programmes with participating cyber / security firms should be considered to help build skills. This eases the problem around the global cyber security skills shortage.

In this regard, KryptoKloud assists with the training of junior cyber analysts who then work for the colleges or universities for a given period of time – enhancing their technical teams.

"It's a good development opportunity for the apprentices – who gain real world cyber experience in cyber operations as well as receiving a great apprenticeship with a Level 4 Award at the end. Without doubt, this is a great return on investment for both colleges and universities."

In addition, there are some key takeaways for all public sector organisations thinking about improving their defense:

- Have an Incident Response (IR) plan in place. Lincoln College made up for their lack of a formal plan with a clear, senior management structure that allowed the CEO to make quick decisions – following the advice of their IR provider. Not all organisations are so lucky; if there are several stakeholders acting independently it can significantly hinder the speed of response. This can be avoided by agreeing on the internal 'people' component of the organisation's IR plan beforehand.

- Consider using a Managed Service Provider (MSP). For many public sector organisations, it will be more efficient both operationally and financially. Many organisations purchase from a vendor (install the software) and think they've done enough, but it's not just the tech, it's the processes and people involved that are extremely important and add the value.

- Do your homework on providers. Much like a garage, it is often not until things go wrong that you know whether you've chosen a good one. But there is support available. The National Cyber Security Centre provides guidance within the public sector and will have a list of recommended providers as does the newly formed regional Cyber Resilience Centres. In addition, the Institute of Directors (IoD), although a private sector-oriented institution, also has a wealth of information available.

Of course, getting the right technology is also important, but a good managed service provider will be able to support you with that. KryptoKloud utilises F-Secure technology because they recognise the quality of the products.

"We're an independent service provider so we do our own analysis of the different vendors and F-Secure's tech comes out head and shoulders above the rest," says Paul.

KryptoKloud has built out its MSP offering using F-Secure technology and has even taken a lead on sharing what they've learned with other partners trying to do the same.

F-Secure Elements has been designed specifically to support partners with building out an MSP offering. It is our all-in-one cyber security platform that lets partners build and manage services more efficiently, by putting everything into a single console.

Click here to learn more about KryptoKloud

Learn more

KryptoKloud | F-Secure