MSPs: STRATEGIC SECURITY ROLE IN MAJOR INDUSTRIES

June 2019

MSPs ARE ON THE FRONT LINE

Cybercriminals are attacking MSPs as a way to get access to their customer base. MSPs are also increasingly involved in supporting supply chains of major industries where the weakest link will be targeted. They need to understand the transactional nature of the market as well as any special regulatory or compliance issues. At the same time, MSPs are being called upon to support customers' IT staff with tools such as Dark Web monitoring, which looks at the various layers and interlinked businesses within a client's network. Backed with a solid understanding of the special threats in a particular industry, the MSP can be in a strong position as a strategic advisor.

The advisor role is a powerful one: MSPs support all parts of the organization while increasing use of cloud and other services by the customer makes the problems of security less directly manageable. The MSP can provide solutions to enhance security awareness across the organization and make all employees more aware.

MSPs are becoming pro-active – with monitoring and helping with risk- assessment. The MSP can provide industry and sector-specific guidance, not only just from a regulatory or a fine perspective, but looking at the impact on reputation and with a response based on infrastructure strengthening.

Cybercriminals are attacking MSPs as a way to get access to their customer base.

MSPs OFFER SPECIAL FOCUS

It is clear from breach reports that certain sectors of industries and types of organizations are coming under repeated and concentrated attacks. If you are an MSP working with clients or potential customers in any of these sectors, you need to pay particular attention to them. You will allso need to understand what the implications there are for you as well as your customer.

The first of these sectors is accounting, where the nature and scale of the data being stored, as well as the compliance requirements, mean special attention is required. This will only ramp up this year with higher personal privacy legislation coming in across Europe and the US.

In a wider sense, the whole financial services industry is being challenged worldwide; there are differing requirements for compliance across global markets, while at the same time this industry is such an obvious target. The financial sector as a whole stands out as being in the forefront of the attacks and having to take special interest in security.

The energy sector is dominated by some giant companies, but the threats are now targeting the smaller businesses who supply them, seeing this as an easy way in and having a potentially devastating impact on a country's infrastructure. Both the energy giants and their suppliers are investing heavily in forms of cybersecurity.

NICK STREAKER | CTO

Nick Streaker (left) leads the shaping and development of ID Agent's technology vision in providing actionable insights to clients across the emerging threat landscape.

He is responsible for the team tasked with development, quality assurance, operations, hosting, product management, and customer technical support. Nick began his career as an intelligence analyst in the US Army. He held a variety of roles during his service in the Army; primarily focused on intelligence analysis as an Arabic and Chinese Mandarin linguist.

He then transitioned to the Civilian Sector as an Enterprise Architect in support of the Department of the Army's intelligence mission. Most recently, Nick was instrumental in the development of an assessment methodology which helped inform Lloyds of London risk decisions in underwriting cybersecurity insurance policies for US Critical Infrastructure. Nick led the development and implementation of a SaaS platform leveraging this methodology to enable the assessment and visualization of cybersecurity risk, culture and maturity across the enterprise. He has presented to both the financial and insurance sectors in the US and UK on the topics of risk and cyber resiliency.

MAKING IT WORK

ID Agent's CTO Nick Streaker says MSPs should adopt a holistic view to security, covering not just the technology, but the changing internal and external threats and the attitudes of the real people in the customer organization. MSPs are now on the front line of security and coming under increasing threat themselves, he adds.

The reality of the situation is that one of the most widespread and easily accessible attack surfaces within organizations is the people they employ. A customer may have large security resources at a certain level to protect the technology, through a firewall, access control to IP and antivirus and malware, but the most widespread attack points are at the employee base.

Providing security training and awareness, as well as phishing simulations, is probably one of the best ways to sensitize an employee base to the significance of the role that they play from a security perspective.

A holistic approach to addressing all of those areas is what is needed by the MSP: identifying the internal and external threats, then the technology, plus the people.

"And this is what the best MSPs are doing. At the end of the day a lot of these breaches are a result of core security fundamentals not being addressed. No matter how sophisticated or how complex the attack mechanisms and how they are delivered, it still relies on this core security," he says.

MSPs are the front line: if a cybercriminal hits an MSP they get access to the entire MSP base and all the end points they are responsible for. This has become particularly noticeable this year and is a pervasive trend that is global in nature, he says.

A holistic approach is what is needed by the MSP: identifying the internal and external threats, then the technology, plus the people.

Looking at the MSPs' level of understanding they obviously have to understand their customer, the nature of the business, and the vertical markets that they're in to understand the security compliance issues. When looking from an industry-vertical perspective it's more about having an understanding from a sales view, looking at the impact and the threat trends against those specific markets.

For an MSP, one of the benefits of being proactive and monitoring what that looks like is showing how to minimize the impact on the customers' business, he says.

"With, for example, breaches such as in personal health information, the MSP would be expected to know what percentage of incidents are associated with that sector. They'll be looking at ransomware trends within that specific industry vertical. And they should evaluate the cost associated with having to recover from that breach. And this should be not only from a regulatory or a fine perspective but looking at the impact on reputation and with a response based on infrastructure strengthening and things like that."

In an industry vertical the MSP is able to discuss the volume, frequency, and the cost associated with breaches in those specific industries. So there's two pieces to the story: the background information like a risk perspective and then the specific regulatory compliance issues that come into play.

"One big challenge for any business operating in European markets is the regulatory obligation. The reporting requirements that are associated with the privacy directive or GDPR means it is vital to be able to articulate to the client their regulatory obligations for reporting."

Looking at the breaches potentially associated with the client themselves means also having the ability to monitor subordinate organizations and supply chain organizations as part of that client base. The client can gain insight into their supply chain through the same mechanism that looks at the internal security.

The Dark Web monitoring service looks at the secondary and tertiary organizations or vendors that users are involved with. It ensures that even if the user hasn't been a victim of a data breach, when these organizations fall victim, the user can potentially identify it before it has been reported.

Basic security products are sometimes a harder sell because of the need to convince the client that they are something they really need. "We've done a couple of things in order to assist MSPs in doing that: one of the most powerful tools is the live search function where even though the results are from a passive perspective and are redacted, it provides real insights for those risk-based decisions."

"IT security staff in particular have a real desire to obtain these types of Dark Web monitoring services because of the value provided from a security posture perspective. This is important in providing an executive level understanding at the client in order for them to make those business decisions to move forward."

And there are other parts of the organization as well as IT involved in decisions. As services are migrated to the cloud, whether it be from HR, payroll, banking and finance, or anyone using social media, collaboration tools, or CRM, there is a need to understand the impact that a breach of any of those third parties would have on the organization.

"One of the most powerful tools is the live search function where even though the results are from a passive perspective and are redacted, it provides real insights for those risk-based decisions."

CONCLUSION

ID Agent's award-winning Dark Web monitoring platform is changing the way MSPs approach security conversations. By leveraging analyst-validated credential exposure data, over 1,700 MSPs worldwide are closing new business and upselling services to existing clients. Only ID Agent provides white-glove sales and marketing support to ensure your success. As a value-added service, ID Agent has developed a Security Awareness Training and Anti-Phishing platform available only to Dark Web ID Partners.

ABOUT ID AGENT

ID Agent provides a comprehensive set of threat intelligence and identity monitoring solutions to private and public-sector organizations and to millions of individuals impacted by cyber incidents. The company's flagship product, Dark Web ID, delivers Dark Web intelligence to identify, analyze and monitor for compromised or stolen employee and customer data, mitigating exposure to clients' most valuable asset – their digital identity.

From monitoring your organization's domain for compromised credentials to deploying identity and credit management programs to protect the employees and customers you serve – ID Agent has the solution.

ID Agent
16701 Melford Boulevard, Suite 127
Bowie, Maryland 20715