timico®

Cyber Security in Retail

Cyber security is a hot topic, and a topic that is often very complicated and overwhelming to those seeking to protect their businesses from attack.

Martin Riley, Chief Technical Officer here at Timico, helps us navigate through the five things that retailers should be considering when reviewing their cyber security infrastructure.

Risk Management

Firstly, understanding risk. Without an understanding of risk, we can't attribute a priority to any activity, and we should be focusing on projects that have a high degree of business impact and increased maturity.

Detection and response

New regulations such as GDPR are imposing real fines on data breaches and as such the business threat goes beyond reputational damage and delivers up to 4% of global revenue. So we have to be able to detect and respond to real and current threats quickly. We need to reduce the breach detection time to minutes and hours not weeks and months.

To achieve this, we need to look at network detection systems across the estate and Security Information and Event Management (SIEM for short) solutions. Technology works even better if your security stack integrates and shares intelligence and activity. This helps provide intelligence and rapid detection of breaches across the broad digital footprint.

This information needs to be fed into a 24 hour SOC for security incident response. Knowing there is an attack means nothing without being able to respond effectively.

Security Rating Services

And lastly, using a Security rating service, you're able to get a real time, continuous and low-cost visibility of the security across your digital landscape.

Where security tooling is well integrated as part of an ecosystem of multiple vendors, security rating services offer an independent view of your maturity by creating a security profile and comparing it to similar companies or even those in the same sector to generate a scoring.

Vulnerability Management

As the landscape sprawls across endpoints, central applications and web services, vulnerability becomes more important. Many vulnerability management solutions come with discovery which help to close the knowledge gaps that occur with virtual machine and cloud sprawl and measure their installed applications again at known vulnerability databases.

Using this information along with knowledge of where or how these systems can be accessed (again, a link to risk management) allows you to identify the areas that need to be patched rapidly or just need to form part of your standard patching policies. Considering that most patching policies stop at the operating system, it is good to have something looking deeper and understanding the vulnerability of infrastructures.

Cloud Access Security Brokers

Whether we're hosting infrastructure in the hyperscaler clouds for customer and internal applications or simply consuming Office 365 and other cloud-based services, you need visibility into what is going on. Cloud Access Security Brokers (or CASB [pronounced Cas-bee] for short) allow us to extend our security policies and visibility into these cloud services and gather data and insight into activities.

For example, working with O365 or cloud-based storage solutions we can create rules for data loss protection and alert us to PII or PCI data being sent or saved somewhere less secure.

Linking in with firewall or endpoint technology, we're able to identify shadow IT and its users to help identify and reduce un-necessary risk.

As a provider of converged managed services, Timico offer Security solutions that can be tailored to specific your business requirements. For more information on how we can improve your organisation's cyber security infrastructure, contact us today.