Deloitte.

Cyber Espionage
A proactive approach to cyber security

#DeloitteRA

To mitigate the risks of advanced cyber threats, organisations should enhance their capabilities to proactively gather intelligence and monitor and remediate vulnerabilities.

Many organisations are still using a reactive, defensive posture to address cyber security incidents. When a security incident is reported, the organisation investigates it and isolates and contains the threat. This is followed by remediation efforts and a root-cause analysis to prevent a reoccurrence of the incident. But such a reactive approach creates enormous opportunities for cyber criminals to both take advantage of known vulnerabilities and search for those that are yet unrealised. New opportunities constantly evolve due to human error, faulty configurations in the infrastructure, flaws in the software, and problems with applications. Advanced cyber adversaries are skilled at locating the not-yet-realised vulnerabilities. And these criminals are increasingly successful in thwarting technology that should protect an organisation.

Why take a proactive approach?

In making the case for a proactive approach, it is essential for CIOs to help executives on the business side understand the breadth of what is at stake and why present-day security controls are only addressing a portion of the issue. Unfortunately, many key decision makers may view taking a proactive approach as an unnecessary and cost-prohibitive effort. Ultimately, a reactive approach allows vast amounts of proprietary information to be easily accessed by undetected criminals. Indeed, this is why businesses are strategic and popular targets. The key to protecting data is performing risk assessments that take into account vulnerabilities that can be exploited beyond those related solely to regulatory compliance. Another aspect of this emerging risk deals with the efficiency of the perpetrators and their holistic approach. Attackers are operating from a business practice standpoint when designing their techniques known as Advanced Persistent Threats (APTs). They are actually taking time and using resources to understand the business processes used by the target entity. Unlike those in place at organisations, there are no standards or governing bodies to control this criminal behaviour – law enforcement is behind the curve because it cannot keep up with the rapid evolution of cyber crime.

Generally, the criminal world has experienced a large shift from an individual, independent focus to a virtual, collaborative model that thrives on innovation and data sharing. Over the past 10 years, a malware ecosystem has formed that supports this wave of cyber crime.

An adversary has an available network of resources from which to choose, and many have specialties. Various groups include criminals from many nation-states (where this work is considered to be a badge of honor), organised crime, hackers, and others. Typically, participants are unaware of the overall mission. Rather, they focus solely on just their portion.

Proactively protecting assets

How do you proactively protect your assets from this burgeoning threat? It begins with understanding the corporate ecosystem, performing a residual risk assessment, and deploying an intelligence-based methodology that converts raw data from internal and external sources into actionable intelligence. It is also important to determine what information, strategic relationships, or behaviours cyber adversaries and other espionage-oriented resources would find valuable. In addition, organisations must review and consider changing the way they structure their business and the way they interconnect with their environment.

Until recently, most organisations have not been taking a holistic view of the security landscape. Cyber threats can come from multiple vectors.

Until recently, most organisations have not been taking a holistic view of the security landscape. Cyber threats can come from multiple vectors. The old standard "point-solution" mentality is no longer sufficient. Security strategies and defenses today require reviewing the entire system and the interdependencies within it. Additionally, anti-virus software is not a complete solution to the problem. It is often ill equipped to disarm many threats, as it deals with technology processes and not the human element behind APTs. The perpetrators of APTs are able to adjust behaviour over time to adapt to changes in the environment, and thereby get the desired result.

When rethinking your approach, it is important first to understand the life cycle of an emerging threat and how the underlying workflow system should be designed and automated to help mitigate an organisation's level of risk from this threat. Data sources and automation can be leveraged for the various phases of the workflow, from proactive planning and detection to response and containment and, ultimately, to remediation and reporting.

Second, organisations need to understand which devices and systems support critical business processes. When planning a proactive defense strategy, anticipate how or if a cyber adversary could exploit these devices and systems. Any device that has an internal computer and is Internet Protocol (IP) enabled, such as cell phones and handheld devices, should be carefully scrutinised for vulnerabilities. Take inventory of devices and components, even those branded under trustworthy names, and determine how the risks associated with them can be addressed effectively.

From reactive to pre-emptive

The cyber threat continues to evolve and disguise itself with ingenious techniques to circumvent most traditional information security programs. Nations around the world continue to advertise and develop cyber warfare capabilities. These programs will provide thousands of future cyber operatives with skills that enable them to thwart traditional security controls. Consequently, the number of individuals and organisations capable of launching attacks using ATPs may likely increase.
To mitigate the risks of these advanced threats effectively, organisations should expand their current capabilities to include proactive, continuous monitoring, while enhancing existing security practices to leverage cyber intelligence.

When rethinking your approach, it is important first to understand the life cycle of an emerging threat and how the underlying workflow system should be designed and automated to help mitigate an organisation’s level of risk from this threat.

Contacts

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Derek Schraader
Risk Advisory Africa Leader: Cyber Risk Services
Mobile: +27 79 499 9046
Email: dschraader@deloitte.co.za

Cathy Gibson
Director: Risk Advisory Africa
Mobile: +27 82 330 7711
Email: cgibson@deloitte.co.za

Henry Peens
Associate Director: Risk Advisory Africa
Mobile: +27 82 496 8694
Email: hpeens@deloitte.co.za

Graham Dawes
Chief Operating Officer: Risk Advisory East,
West & Central Africa
Mobile: +254 71 989 2209
Email: grdawes@deloitte.co.ke

Tope Aladenusi
Partner: Risk Advisory Africa
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Designed and produced by Creative Services at Deloitte, Johannesburg. (000000/jo)