Creating a GDPR Compliance Framework with security tech

By Pieter Engelbrecht

26 Mar 2019

There has been a lot of talk of GDPR over the last year, so organisations today understand the serious repercussions of non-compliance and many have put basic frameworks in place with a focus on two pillars - 'people' and 'process'.

Pieter Engelbrecht, Business Unit Manager, Aruba HPE

People - GDPR stipulates the appointment of a data protection officer (DPO) for any organisation that is a public authority that has a core activity involving the monitoring of individuals on a large scale, or the processing of large volumes of sensitive data. The DPO needs to have a thorough knowledge of GDPR and have an independent voice within the organisation.**Process** - Many organisations' GDPR approach so far has been data mapping – identifying where, why and how personal data is being used, while also eliminating any unnecessary data processing. Once this is done, each organisation has a foundation from which to ensure secure policies and processes are in place.

While the two GDPR pillars – 'people' and 'process' have been looked at, there has been a bit of lag in the use of the third pillar - 'technology' – which plays an important role in detecting attacks and crucially, responding to attacks. Do organisations need to rip and replace existing cybersecurity tools?

Let's look at the technology aspects of data protection and GDPR:

Technology: Security solutions to the rescue

A GDPR security strategy should look at 4 technology areas. By applying good quality security solutions to each of these areas, security teams and the DPO can together manage the inevitable exposure to the risk of cyber attack:

Network Access Control (NAC)

Businesses today embrace the idea of anywhere, anytime connectivity, but have largely ignored the need for secure NAC. Many employ a laid-back "connect now, secure later" NAC philosophy. Others simply choose the same vendor for security that they use for network infrastructure. Both of these approaches give the illusion of security - even compliance - but in reality, leave extensive security gaps.

Network access control (NAC) offers, at a minimum, authentication of a user or device. With mobile access now the norm and Internet of Things devices connecting to the network, the only way to ensure proper access is maintained is to go beyond simply validating credentials. The next level beyond this is to tightly control who and what is authorised to access IT assets, including personal information.

With advanced NAC, the IT team knows where personal data is located. They can use NAC to stipulate who is entitled to access that information and under what circumstances. In an ideal world, NAC and policy management solutions will provide device discovery, role-based access to IT assets and a closed-loop, policy-based attack response. For complete convenience, it should also integrate seamlessly with existing network infrastructure, perimeter security systems and service and support offerings.

Assurance

The next level of protection relies on the fundamental security of the underlying network infrastructure. If data can be easily tapped off the network in normal day-to-day business flows and process, the chances of a breach increase.

This is where technologies such as equipment tamper-proofing, encryption, key management and secure network administration are critical to the overall security strategy.

Breach Detection

GDPR requires the reporting of a data breach within 72 hours. Many existing systems can take almost all of this time to detect and generate the required event information.

While prevention is better than cure, early detection of a breach is a close second. There's a huge range of different technologies and products available that find attacks before they do damage.

Today more and more attacks are specifically designed to breach traditional defences. It is because these exploits almost always result in the loss of personal information (and a quick sale on the Dark Web) that new approaches to attack detection are required. For example, a high volume of breaches makes use of valid credentials, which means phishing attacks and social forensics are one of the biggest risks.

The result is the bad actor using legitimate credentials to execute an attack that may take days, weeks or even months to unfold.

How do you stop an 'attack' using valid credentials to tap information the real user has a valid reason to access? Because these are previously unknown attacks, it's no use to look for a signature or pattern to detect them.

This means IT and security teams introducing an additional level of monitoring that complements existing defences, one that uses new types of attack detection such as machine learning to detect small behavioural changes that suggest an attack has occurred. Actions can range from requiring re-authentication or quarantining to totally blocking network access.

Machine learning can establish a ‘risk score’ based on the characteristics of suspected unusual behaviour and how these characteristics differ from the norm. This helps organisations to prioritise their resources and investigate suspected attacks before they do damage.

Response to Breach

The GDPR’s breach notification requirements are very clear when it comes to what an organisation must do when a personal data breach occurs. These include notifying the regulator within 72 hours of being ‘aware of the breach’ and notifying impacted individuals ‘without undue delay’. The notifications must include details of the breach including:

- The type of data, type of exposure and the number of individuals involved
- The probable consequences of the breach
- Any mitigation actions taken

So, in the unfortunate event that a breach occurs, the DPO and his team need to rapidly gather the facts: what happened, the scope of the damage, and a plan of containment and remediation. This all has to be communicated to the regulators and authorities in a clear, concise manner. It is vital they have the tools and solutions to deliver this information efficiently. Any delays in gathering this information could cost the organisation dearly, both reputational and financially.

In conclusion, GDPR ‘compliance’ is not fully defined by the law and will be determined in part by rapidly advancing security technology capabilities and evolving best practices. Only technologies that are open and interoperable will make it through to the next generation of cybersecurity defences.

**Pieter Engelbrecht was interviewed by Pieter Engelbrecht.*

ABOUT PIETER ENGELBRECHT

Pieter Engelbrecht is the business unit manager at Aruba, a Hewlett Packard enterprise company.
- How autonomous IT and security solutions will enable proactive IT departments - 11 Apr 2019
- Creating a GDPR Compliance Framework with security tech - 26 Mar 2019
- Why are CIOs and CISOs positions becoming more challenging? - 31 Oct 2018
- Mitigate WAN complexity with SD Branch - 18 Sep 2018
- Securing the enterprise network with artificial intelligence - 21 Nov 2017

View my profile and articles...