WHITE PAPER

ARUBA SECURITY SOLUTIONS FOR GDPR

A 360-DEGREE VIEW OF PEOPLE, PROCESS AND TECHNOLOGY

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

INTRODUCTION

No matter what the objective or task, organizations operate best with a well-tuned mix of people, process and technology, and this is especially true when implementing cyber security protection. Cyberattacks have become more targeted, more organized and more lethal. With the advent of mobile connectivity, cloud and IoT, these attacks have a much easier time finding gaps in cyber defenses and making their way inside the network.

As a result, governments and industry regulators have become increasing more comprehensive in specifying how organizations implement cyber security, especially as it relates to personal information. In Europe, a new privacy regulation, known as General Data Protection Regulation (GDPR) introduces a gold standard for data protection and will impact any organization (independent of location) that maintains European personal data. Other governments worldwide are adopting similar approaches, so preparing for data privacy regulations is a global responsibility.

The EU data protection laws passed in the 1990's led the way in assuring the rights of individuals to control the collection and use of personal information. These are being further enhanced with the passing of the GDPR, which comes into effect on May 25, 2018. The goals of GDPR are:

"….to harmonize data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organizations across the region approach data privacy."

While GDPR has gained a great deal of attention from the potentially significant financial penalties that can be imposed in the event of a loss or misuse of personal information, what is equally important is the prescriptive nature of the regulation. It will require organizations to invest in preparing people, and adopting new processes and technology, to comply. The GDPR covers a wide range of topics and activities from record keeping, individual rights to access, delete or port data, security and security breach notification.

This purpose of this document is to focus on how cybersecurity products and technology can assist organizations with GDPR compliance.

PEOPLE—THE DATA PROTECTION OFFICER

An important element of GDPR is the role of the Data Protection Officer (DPO). Any organization 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, must appoint a DPO.

The DPO must have specialist skills and expertise and be involved in data protection issues. A DPO sits at the crossroads of business processes, IT systems, security and has knowledge of GDPR to ensure that an organization is in compliance. In fact, the regulation makes a strong point about the need for the DPO to have an independent voice and influence in the organization.

The DPO will need to engage with the security team or function in three key activities:

1. Monitoring compliance with GDPR, including collecting data and information about processing activities to ensure proper protection is in place and is effective.
2. Facilitating and reviewing a data protection impact assessment of new projects that collect and utilize personal information, including an evaluation of the proposed security controls.
3. Providing a central point of communication and mediation in the event of a data breach, including complying with very specific requirements for the timing and content of communications with the regulators and affected individuals.

As a result, while the DPO does not have direct responsibility for the implementation and management of cyber security defenses, he or she must have full knowledge of how the systems, networks, applications and databases are being protected from attacks, what information and data they will provide in the event of a breach and a level of confidence that these safeguards will lead to GDPR compliance.

PROCESS—FINDING, INVENTORYING AND RATIONALIZING PERSONAL DATA

Most organizations have conducted data mapping exercises as a key part of their GDPR compliance programs. The goal is to identify where, why and how personal data is being used and eliminate the processing of data which is not necessary. This "housecleaning" exercise then provides a foundation from which to ensure policies and practices are in place to manage and protect the data.

The resulting personal data inventory and rationalization process turns out to be of tremendous value in designing the security mechanisms required to protect it. When IT and security teams can pinpoint the location, application and storage techniques for personal data, they can design and implement the security processes and technologies that the DPO will need to see, understand and interact with to fulfill his or her mission.

TECHNOLOGY—SECURITY THAT KEEPS PACE WITH THE ADVERSARY

No matter what the size or industry, organizations are under continuous attack—almost always with the goal of either stealing business or personal data or, in the case of Ransomware, rendering it unusable.

While no single product or combination of security solutions will guarantee GDPR compliance, there are four areas that merit attention in establishing a level of security appropriate to the risks:

1. Access
2. Assurance
3. Detection
4. Response

With the appropriate application of security technology to each of these areas the security team can be a strong ally of the DPO in managing GDPR security and the financial exposure associated with a breach.

Access

Many organizations have implemented some form of network access control (NAC) that, at a minimum authenticates a user or device. With increasing mobile access and the influx of "things" such as cameras, vending machines, medical equipment, etc. connecting to the network, the only way to ensure that proper access is maintained is to go beyond simply validating credentials to tightly controlling who and what is authorized to access IT assets such as personal information.

Now that the IT team knows where personal data resides, they can use NAC to stipulate who is entitled to access that information and under what circumstances. For example, in a hospital, nurses and doctors may have access to patient records, but finance staff or heart monitors will not. This means that at time of network entry, the attack surface is reduced by restricting the number of people (and devices) that can execute a breach.

Assurance

Once user access is established, the next level of protection relies on the fundamental security of the underlying network infrastructure. If data can be easily siphoned off the network while it flows to support key business processes, 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.

Detection

There are many different technologies and products to find attacks before they do damage. Traditional security defenses rely on pattern matching, rules and signatures to find malware and other threats that have been previously seen and understood. In most cases, products that use these techniques are effective and will remain essential in protecting the organization. In fact, any new technologies should seamlessly integrate with what is already in place.

However, in the past several years, attacks have been designed specifically to evade these products and their success can be seen in the constant barrage of breaches that make the headlines. It is because these exploits almost always result in the loss of personal information—with a ready market on the Dark Web—that new approaches to attack detection are required. Whether it is a user that has opened the wrong email attachment or a rogue insider, the result is that the bad actor is using legitimate credentials to execute an attack that may take days, weeks or even months to unfold. Because these attacks have never been seen before, looking for a signature or pattern to detect them will not work. This means that IT and security teams are introducing an additional level of monitoring that complements existing defenses, one that utilizes new types of attack detection such as machine learning to find small changes in behavior that are indicative of an attack.

Response

The GDPR introduces breach notification requirements that are very prescriptive in terms of what an organization is required to do when a personal data breach occurs that presents a risk to individuals. 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:

- scope of breach: type of data, type of exposure and the number of individuals involved
- likely consequences
- mitigation actions taken

In other words, in the unfortunate event that a breach occurs, the organization must rapidly understand what happened, the scope of the damage and form a plan of containment and remediation—while communicating all of that in a clear, concise manner with the hopes of avoiding significant penalties. The DPO must be involved to help assess and manage the breach notification requirements.

As a result, the IT/Security team will play a critical role in managing a breach, including assembling and communicating critical information about the breach in a very short period of time. So, it is important that they have the tools and solutions to deliver this information efficiently.

A FOCUSED SECURITY SOLUTION: THE ARUBA 360 SECURE FABRIC

Aruba provides an integrated set of security products and technologies that can help support any organization's GDPR compliance programs.

The Aruba 360° Secure Fabric gives security and IT teams a simpler way to plan for, detect and respond to advanced cyberattacks across multi-vendor infrastructures, supporting a wide range of enterprises and securing anywhere from hundreds to millions of users and devices.

Here are how the components of the Aruba 360 Secure Fabric map to GDPR imperatives:

Access

Aruba ClearPass is a robust secure network access control (NAC) and policy management solution providing device discovery, role-based access to IT assets and closed-loop, policy-based attack response. ClearPass integrates seamlessly with both Aruba and existing IT and security solutions through built-in integration with other vendor's network infrastructure, perimeter security systems and service and support offerings. As a validation of ClearPass' maturity and inherent security, the product has achieved the most comprehensive Common Criteria certification of any access control solution on the market.

Assurance

Aruba Secure Infrastructure features essential security capabilities embedded in all the Aruba Wi-Fi access points, switches and wireless controllers. With Aruba networking products, IT administrators can be assured that network devices and the traffic that flows through them have not been compromised. In combination with ClearPass, Aruba wired and wireless networking solutions deliver precision control over who, what and how users and devices can access personal information.

Detection and Response

The Aruba IntroSpect User and Entity Behavior Analytics (UEBA) solution is a new family of continuous monitoring and advanced attack detection software that uses machine learning to spot small changes in behavior that often indicate attacks on the inside of the network that have evaded traditional security defenses. Machine learning algorithms create a risk score based on the maturity and severity of an attack to prioritize incident investigations for security teams so that gestating attacks are detected and stopped before they do damage. To align with GDPR, IntroSpect also leverages the knowledge of where personal data resides to increase a risk score for systems or databases that might be involved in an attack—focusing the attention of IT and security on critical potential data breaches.

Once an attack or breach has been detected, IntroSpect accelerates the incident investigation and evidence accumulation process to enable the IT team to provide the information required for the DPO to report to the Supervisory Authority while complying with the other GDPR directives.

In addition to helping with breach management, IntroSpect is highly integrated with ClearPass to utilize ClearPass' role as "gatekeeper" of the network to initiate pre-determined, policy based actions in response to attack. Actions range from requiring re-authentication, quarantining to totally blocking network access.

Good IT Citizenship

The Aruba 360 Secure Fabric is open and multi-vendor. This means that organizations can use any of the 360 Secure Fabric elements without requiring the others and then add on as needs evolve. In addition, the Aruba 360 Security Exchange technology partner ecosystem consists of more than 120 leading security and IT providers who collaborate with Aruba to offer pre-integrated, best-in-class enterprise security solutions. As a result, existing investments will not only be maintained, they will be enhanced with the additional value that integrated Aruba security solutions provide.

SUMMARY

The EU continues to raise the bar for personal data protection and influence the development of privacy laws throughout the world. The size of the potential fines under the GDPR has created added focus for organizations on ensuring their security practices are robust and continue to improve in order to address the growing sophistication of threat actors. GDPR "compliance" is not fully defined by the law and will be determined in part by state of the art in security technology and evolving best practices.

No matter how GDPR progresses, cyber security will play a pivotal role in compliance. Security and IT teams now have the opportunity to use the GDPR framework to better manage the collection and use of personal data while filling in potential gaps in their protection infrastructure. The good news is that solutions like Aruba's ClearPass for secure network access control and Aruba IntroSpect UEBA, can deploy alongside current security solutions, contribute to GDPR compliance, improve overall security and help organizations reach the level of protection that the EU regulators are seeking.

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives. For more information visit www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Community at http://community.arubanetworks.com.

For more information, go to http://www.arubanetworks.com/solutions/security/

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com