RES

HOW TO MEET THE NEW MANDATES FOR EUROPEAN CONSUMER DATA

Five Security Strategies for GDPR Compliance

Today's consumers are not happy. Cybercrime is a growing and profitable business, fueled by criminals who are learning ever more creative ways to thrive on exploiting valuable consumer data. And demands for more secure keeping of personal data is awakening governments around the world to the importance of data protection, driving them to tackle the problem with ever more stringent legislative solutions.

But protective legislation puts increasingly heavier burdens on those who collect customer data, meaning that — once again — enterprise IT must discover new ways of resolving the conflict between regulatory compliance and business productivity.

This paper looks at the most significant example of recent legislation, suggesting practical and innovative solutions for IT that can relieve the pain and cost of regulatory compliance.

OUCH!

When it comes to regulation, it's hard to beat the European Union (EU). In May 2016, the EU – famous for the bendy banana law that legislates acceptable banana curvature — enacted Regulation 2016/679[i] for "the protection of natural persons with regard to the processing of personal data and on the free movement of such data...." Known as the General Data Protection Regulation (GDPR), it replaces pre-existing EU regulation, standardizing and toughening security laws governing consumer data. GDPR introduces:

- Sweeping requirements for granting much greater personal control of data by EU citizens
- Detailed notification requirements when data breaches occur
- The need for organizations to hire "data protection officers" focused on protecting consumer data
- Much heavier fines for organizations found in breach of GDPR regulations

While GDPR doesn't take effect until May 2018, it requires substantial changes to organizational and IT infrastructures that won't be quick and easy to accomplish. And the costs of noncompliance with GDPR include stringent fines, penalties[ii] and compensatory damages for infringements[iii] . Administrative fines alone for noncompliance with certain GDPR provisions can be up to 20 million Euros or 4 percent of a company's total worldwide annual revenues. "Ouch" indeed.

While GDPR doesn't take effect until May 2018, it requires substantial changes to organizational and IT infrastructures that won't be quick and easy to accomplish.

The potential for such tremendous financial impact has more than EU financiers salivating. Corporate insurance underwriters are taking seriously their assessments of GDPR compliance as a source of substantial risk when calculating an organization's insurance premiums.

Timely GDPR compliance for companies doing business with EU-member countries isn't an option. The stakes are high. And time is running short.

THE UNHOLY QUINTUMVIRATE:
5 SECURITY CHALLENGES THAT KEEP YOU AWAKE AT NIGHT

GDPR is clear about the need for security requirements to protect customer data, but it is less specific about exactly what organizations need to do to secure personal data. Although the road to compliance may be different for every organization, most should focus on implementing new methods for reducing the security vulnerabilities resulting from these five IT headaches:

1. Mobile workers who want to connect from anywhere at any time
2. Privileged users who need admin rights to an astonishing variety of systems
3. Costly and predatory impacts of ransomware and malware
4. Risks of employee onboarding and offboarding
5. Audit trails: the tracking and reporting of personal data access

Is that enough to disturb a night’s sleep? Fortunately, it’s the nature of technology to provide solutions for every complex challenge. We’d like to share with you five readily available and quick-to-implement security strategies that you should consider adding to GDPR compliance plans.

#1:
“I NEED IT RIGHT NOW!” HOW TO DECREASE SECURITY EXPOSURES FROM MOBILE WORKERS.

Mobility = productivity. Enabled by ubiquitous wireless connections and cloud-based apps an d services, mobile workers are dominating the business landscape — as well as IT roadmaps. But each mobile device and access point dramatically increases the opportunity for intrusion into the enterprise infrastructure by malicious operators.

For years, IT has developed tremendous perimeter-based static security technologies – only to see them neatly circumvented by an eager worker tapping on a smart phone while connected in a corner coffee shop. To protect organizations from these new risks and help ensure GDPR compliance, new context-aware security and policy controls are a must.

Context-aware controls dynamically adapt each worker’s digital workspace to the level of security risk they pose based at any given time based on their working criteria:

- Are they connecting with a known or unknown device?
- Are they connecting via a trusted or untrusted network?
- Are they using unrecognized or company-sanction USB drives or peripherals?
- Are they attempting to access sensitive information during business hours or at an unusual time of day?

With these context-aware access controls in place, IT can easily control and track worker access — as well as create audit trails that assist in meeting GDPR compliance requirements.

#2:
“BUT I NEED THOSE ADMIN RIGHTS!” TAKE BACK CONTROL OF PRIVILEGED USER ACCESS.

Organizations need to be able to grant and remove elevated IT access rights to users as needed to keep their business productive. But privileged users aren’t just IT administrators; they can also be, for example, workers who need to download apps and are granted full domain rights instead of limited access to only the resources they need.

Organizations need to be able to grant and remove elevated IT access rights to users as needed to keep their business productive.

For the sake of expediency, some organizations grant elevated access rights to almost everyone within the enterprise simply because they lack the resources and capability to govern that access more cautiously. In most organizations, “least-privileged user” access policies are often met with uncomfortably liberal standards. But every privileged user is a prime target of malicious actors, increasing vulnerability because their elevated access rights allow attackers to more easily navigate corporate networks, systems and applications.

Dynamic access controls can automatically elevate and reduce access as needed to allow users to efficiently conduct their work while reducing security risks. With dynamic controls, privileged user rights can be immediately reduced when administrators or others move out of an application or indicate a job is complete. Every reduction in user privilege reduces the risk of security breaches. Putting dynamic controls in place can have tremendous impact on achieving GDPR compliance.

#3:

NO, IT'S NOT REALLY THE FBI! CONTAIN RANSOMWARE AND MALWARE ATTACKS.

Ransomware and other malware will have zero impact on your organization — if they can't get in. And their most likely means of access are email phishing attacks. Attackers also use websites and external drives and peripherals to transmit malicious code to devices and gain access to personal data. Devices become infected when workers click on an email link, visit compromised websites or connect to USB flash drives obtained from third parties. By taking proactive measures such as whitelisting and locking down website and file access, organizations can reduce their exposure to attacks.

Whitelisting allows only approved executables to be opened. Most organizations already have some form of whitelisting in place, but adding granular hash-level controls that employ signatures to open files or execute applications will go a long way towards helping prevent users from accidentally launching an attack when clicking on a link or email attachment.

Organizations can also put controls in place to dynamically block users from accessing specific websites or files, to prevent users from saving malicious files to local drives or disks, and to lock down external devices so only protected or encrypted files can be opened or saved. Proactive controls help organizations ensure personal data is protected and demonstrate compliance with GDPR security requirements.

#4:

SAYING GOOD-BYE SHOULD BE AUTOMATED: SECURE ONBOARDING AND OFFBOARDING.

Many organizations still rely on manual processes to onboard and offboard workers, which often leads to inaccuracies and delays of days or weeks. A recent Ponemon Institute study found that more than 24 percent of people leaving an organization still had access to their corporate data even weeks later.[iv]

IT processes can automatically provision workers with role-based access to the apps and services they need to do their jobs. And the same technology can be used to immediately de-provision workers the moment they leave the company, or move or change roles. Automating provisioning and de-provisioning enforcement policies are more secure, and they dramatically ease the task of IT audit preparation.

Provisioning and de-provisioning processes should be tightly integrated into existing human resource apps, project management systems, or other enterprise identity stores, so access changes can be automatically triggered when a worker's identity status is changed in those systems. With this more holistic approach to identity lifecycle management, organizations can significantly improve productivity and security while supporting GDPR compliance requirements.

> With this more holistic approach to identity lifecycle management, organizations can significantly improve productivity and security while supporting GDPR compliance requirements.

#5:

YOU DID WHAT? WHEN? LOG AND TRACK ACCESS TO PERSONAL DATA FOR ACCURATE REPORTING.

Organizations must maintain records of all processing activities, easily reporting on personal data use and processing compliance. Who accessed what data must be tracked, and organizations should be able prove that proper controls have been implemented to secure personal data.

Logging technologies can track activities and satisfy auditor requests without hassles. They should also be able to easily produce reports about deployed workspace details including changes, usage, devices, apps and configurations. Log tracking and reporting will allow organizations to demonstrate proof of GDPR compliance and quickly prepare the information required for reporting breaches to supervisory authorities and individuals.

YOUR GDPR CHALLENGE:
HOW RES CAN HELP

Organizations have until May 25, 2018, to update their frameworks before new GDPR rules are enforced. But achieving compliance can be made much easier by taking a people-centric approach to security and access management practices. By focusing on governing individual access to systems in a dynamic and less obtrusive way, GDPR compliance can be achieved with much less disruption to worker productivity — and less risk of non-compliance penalties. This means making application and access controls context-aware, and protecting workers from inadvertently introducing threats into their environments.

RES ONE Security can help organizations meet GDPR requirements and strengthen a data protection strategy in several key areas:

- **Provisioning and de-provisioning** — automatically grant access to apps and services based on technology and business triggers; then avoid security risks by automatically removing access if a worker changes roles or is no longer with the organization.
- **Identity management** — align user roles and functions to the appropriate qualifications for delivering access to apps and services.
- **Context awareness** — manage access rules based on granular contextual conditions including person, location, device, time of day and other criteria.
- **Device lockdown** — control what workers can and cannot do on a particular device based on their individual contexts, and extend security by integrating with mobility management systems.
- **Dynamic privileges** — designate who can execute specific administrative tasks within an application without granting full administrator rights.
- **Audit tracking** — leverage log reports to prove to auditors that access and policy controls are in place, and identify where data is or is not accessed.
- **Whitelisting and blacklisting** — implement granular whitelisting and blacklisting to defend against ransomware and other malware, and control which apps and files can be executed.
- **Workspace restoration** — ensure worker productivity with the ability to fully restore a workspace, based on each worker's profile, after an endpoint has been compromised.

With RES, GDPR compliance doesn't have to come at the cost of worker productivity or experience.
To learn more, visit www.RES.com/Security.

SOURCES

[i] http://eur-lex.europa.eu/eli/reg/2016/679/oj

[ii] http://eur-lex.europa.eu/eli/reg/2016/679/oj, Articles 83 & 84

[iii] http://eur-lex.europa.eu/eli/reg/2016/679/oj, Article 82

[iv] http://media.techtarget.com/Syndication/NATIONALS/Data_Loss_Risks_During_Downsizing_Feb_23_2009.pdf

ABOUT RES

RES creates, automates and secures digital workspaces to improve the experience and productivity of the workforce while lowering IT costs. RES takes a people-centric approach to making technology access secure, even in complex multi-device/multi-location scenarios, across physical, virtual and cloud environments. RES boasts numerous patented technologies, fast time to value, and superior customer support for more than 2,500 companies around the world. For more information, visit www.res.com, contact your preferred RES partner, or follow updates on Twitter @ressoftware.

v 1.0 01/06/17