Cloud Act, Patriot Act, GDPR
How can you protect your sensitive data?

Interview with Philippe Anel,
CTO at Mediawen

When we hear “data security”, our thoughts often leap straight to methods to prevent hacking and theft by people with malicious intentions. But that’s only one part of the story. Now more than ever, the rise of mass data analysis by what is clumsily referred to as “artificial intelligence”, or more correctly, “machine learning”, gives rise to another problem.

Indeed, the data requiring protection is no longer merely the product of a company’s work, which could be stored in a safe. The issue is no longer to protect the secret chemical formula that will change the world at all costs.

Today, the most valuable data is data collected about people and the way in which they use a product, service or piece of information on a daily basis. This data is worth its weight in gold and can be used to harm an individual or even a whole group of people.

These new algorithms, boosted by computational power and the extraordinary quantity of data collected, reveal who you are in statistical terms often better than you could even describe yourself [1].

That means it is now essential for companies to be able to explain how they use the data they collect when they create a service and for what purpose. We entrepreneurs use this data, and we must provide information about how we protect it. This shows respect for our clients and inspires their trust.

Implementing standards, good practices, GDPR.

The purpose of a company is to sell, and if possible, to do so quickly. Sometimes, this comes at the expense of securing the company’s services, because they haven’t yet grasped the importance of doing this: “oh, we’ll see about that later”. But make no mistake: customers are becoming increasingly aware of the importance of protecting their personal data. And since the GDPR came into force, they’ve been making this known to companies.

People are starting to wake up, as worrying information continues to emerge, even in April 2019, that Facebook has kept millions of passwords unsecured, for example [2] [3].

This follows the scandals surrounding the American elections and ongoing criminal investigations into the use of data, in which Facebook has been implicated [4].

Users and customers are right to inform themselves. They have adopted fashionable terminology, such as “compliance”, which means ensuring that security standards are met. Growing awareness of the importance of data security prompts us to identify good practices and better methods. And there are plenty.

This process encompasses several areas: raising awareness among company staff, contractual obligations and technical considerations. On the customer’s side, there are two types of sensitive data: the first data in need of protection is raw data, processed content. But the personal data belonging to the

customers or users of a service is no less important. And things don’t get any better when governments get involved.

Cloud Act - Patriot Act, same old story?

The Patriot Act [5] allows government agencies in the USA, including the NSA, CIA and FBI, to obtain information as part of investigations into terrorism. This law only applies to data stored on servers in the United States. It seems legitimate given the international context we currently live in.

But the Cloud Act [6] is something quite different. Ratified by Donald Trump on Friday 23 March 2018 [7], it allows access by the American authorities to electronic data stored abroad as part of a legal investigation. American authorities in possession of the relevant warrant can therefore ask a service provider governed by American law to supply your data, even if it is stored on servers hosted in Europe. They don’t even have to inform you!

Doesn’t the GDPR protect us from the Cloud Act?

The GDPR can’t do anything about this practice. A company or service provider governed by American law will submit to American jurisdiction, even when the rules of the GDPR apply to it. In theory, companies based in Europe could refuse to cooperate. But in reality, this is far too risky for their own image: they could be held responsible in the event of a terrorist attack, for example, or accused of protecting criminals. And that could be bad for business. [8]

Good practices for securing your company data

To secure your company data, you must first be aware that the biggest risk comes from within. We’re not saying you should be suspicious of your employees. But when you’re aware of the true value of data, it’s easy to see why limiting access to it is a logical step to take.

Valuing data includes recognising the risk involved in losing it. In general, we only fully understand the risks when it actually happens: a computer or telephone is stolen, a hard drive refuses to reboot, someone accidentally deletes everything... The solution to data loss is simple: data backups and redundancy in remote geographic locations.

But by increasing the number of backups and storage spaces, you're also increasing the risk of theft. Cryptography is a useful tool to consider in order to enhance data security, providing the means to deal with the computing power now available to everyone and with the impending arrival of quantum computing.

If “legal” access to your data, authorised by the Cloud Act or the Patriot Act, is a disincentive to your customers, the best thing to do is to pay for your data to be hosted by a European company in Europe. If you choose this option, you’ll have to ensure that the company is not bought or funded by an American company, which would allow the extraterritorial right of access to your data. Digital sovereignty is currently a major challenge for companies. They must have control over their data.

There are also illegal data capture methods like hacking and sniffing. It’s a complex issue. In my view, it’s important for companies to encourage their customers and users to work with updated, secure browsers and operating systems, or even to impose them. I know how difficult that can be. It’s a real bind and updating can sometimes mean the tools used become obsolete.

In terms of development, I take a rather extreme standpoint. It's important to avoid ready-made frameworks which are also potential attack vectors. For example, in terms of authentication, if you allow a user to sign in to your site using their Facebook or Google account, how can you ever protect them? Of course, it's quick and easy to set up. But the cost could be far higher if you fall victim to an attack.

When you're low on resources, it's important to prioritise simplicity. Numerous digital security breaches are due to the growing complexity of the tools available. For developers, the article by Russ Cox on software dependencies is very useful [9].

At Mediawen, the use of a dedicated server to store important data such as user data is one of the solutions we've put in place. Virtual machines are certainly cheaper, but they are also shared with other virtual machines. And what we know now about security vulnerabilities such as Meltdown [10] and Spectre [11] on current processors doesn't really inspire confidence. There's no shortage of material on the subject. There's no shortage of patches either...

It's also essential to keep components up-to-date, for example, the TLS protocol which replaces the SSL. Heartbleed-type bugs [12] have also caused a lot of damage. Make sure too to keep track of information about the vulnerability of the entire development process you are using. It's a good idea to update your compilers and tools regularly! [13]

Overall, technological monitoring is essential. Technological independence is also key! The ability to write code which is easy to maintain, well-documented and well-built will allow you to adapt to new attack vectors.

What questions do customers ask?

The questions asked are often simple: "where is my data hosted", "who do you work with?", "do you also offer private SaaS?", "do you offer on-premises software?" (the possibility of installing a service directly onto the customer's server), "how do you ensure data is protected?", "when and how do backups take place?", "can I erase my data at any time?", "can I obtain the data collected about me by your service?", etc.

You'll see that in these circumstances, answering "we'll see about that later" is far from acceptable. Bear in mind that cyber security is a foundation on which you develop your products and services. If you put it off, it's much harder and more expensive to take action later. And in some cases, it can even be too late.

The solution isn't just technical, although that's important too.

It's important to use recent tools to write code, as huge progress has been made in the programming tools and languages available, especially to simplify the work of testing and validation. For example, in the Go programming language [14], which I use increasingly regularly, there's a whole infrastructure for testing. You can find out more by reading the information on this link [15]. These tools are more and more common in all programming languages.

For some time now, new attacks have been using hardware bugs in some microprocessors as vectors, although the issue has received little media attention [10] [11] [16]. These are extremely serious

situations. But it is also possible to protect yourself from them. You just have to equip yourself with the means to do so.

As I said earlier, the use of dedicated servers instead of virtual machines and encryption are excellent solutions. If data is encrypted, it will be more difficult to read, especially if you reduce the attack surface of your server.

Make sure you pay attention to the method you use. Data must be exploited. And to do that, it must be decrypted at some point. If you allow a malicious company to get hold of your cryptographic keys, then all your efforts will have been in vain.

Is there also a legal solution?

It's also a good idea to protect both your own data and that of your users legally. That means using resources which ensure that data confidentiality is respected. In Europe, the GDPR protects user data specifically. Data sovereignty for companies is the biggest challenge at present. You must ensure that your data processing is compliant with security standards, updating it regularly in response to the quickly changing context.

Ultimately, the solution is human and cultural.

Unfortunately, I do not think that the GDPR is sufficient to address these challenges. The strength of the GDPR lies in its ability to raise awareness about the challenges and threats relating to data security. It is pragmatic in its approach.

Compliance also involves raising awareness among employees of companies or organisations through training programmes about confidentiality and data protection. Without this learning and awareness from every member of the company, it will be difficult or even impossible to implement the relevant measures.

The solution also has a political dimension: it will depend on the ability of European governments to maintain a collaborative approach and to create stakeholders who are able to compete with our current leaders. Right now, we're behind. But where will we be tomorrow?

Security, a wide-ranging operation.

All evidence suggests that it is preferable to work with European companies with servers in Europe. That doesn't mean you should shut yourself off to other markets, but it is important that you are able to provide a guarantee to customers that they are protected by legislation.

Customers must know what data they want to protect and possess enough information to help them decide on the compromises they are willing to make. Our role is to explain the measures to be implemented to ensure optimal security, and their consequences.

In order to do this, the first thing to do is to design an application which can be easily moved from one resource provider to another. Modularity and agility are essential to avoid being entirely dependent on a third party and to maintain control over both your data and your company's future.

Philippe Anel, 2019.

Addendum

This article follows an interview published on the Xperteam blog [17]

Philippe Anel, CTO at Mediawen, worked in security with American and Israeli companies (Trustware/ Bufferzone, LANDesk) for more than 10 years, focusing especially on preventing hacking during viral or malicious attacks.

List of links:

[1] https://www.europe1.fr/sciences/Facebook-vous-connait-beaucoup-mieux-que-vos-proches-761818

[2] https://www.lemonde.fr/pixels/article/2019/03/21/facebook-a-conserve-des-centaines-de-millions-de-mots-de-passe-de-maniere-non-securisee_5439366_4408996.html

[3] https://www.lemonde.fr/pixels/article/2019/04/04/les-donnees-de-540-millions-d-utilisateurs-de-facebook-librement-accessibles_5445690_4408996.html

[4] https://www.lemonde.fr/pixels/article/2019/03/14/facebook-enquete-penale-aux-etats-unis-sur-des-acces-partenaires-aux-donnees-des-utilisateurs_5435938_4408996.html

[5] https://fr.wikipedia.org/wiki/USA_PATRIOT_Act

[6] https://fr.wikipedia.org/wiki/CLOUD_Act

[7] https://www.lemonde.fr/pixels/article/2018/03/24/aux-etats-unis-une-loi-vise-a-encadrer-la-saisie-d-emails-a-l-etranger_5275736_4408996.html

[8] https://blog.httpcs.com/cloud-act-et-rgpd/

[9] https://research.swtch.com/deps

[10] https://fr.wikipedia.org/wiki/Meltdown_(vuln%C3%A9rabilit%C3%A9)

[11] https://spectreattack.com/spectre.pdf

[12] http://heartbleed.com/

[13] https://www.cvedetails.com/vendor/14185/Golang.html

[14] https://golang.org

[15] https://golang.org/pkg/testing/

[16] https://fr.wikipedia.org/wiki/Mart%C3%A8lement_de_m%C3%A9moire

[17] https://xperteam.net/cloud-act-patriot-act-rgpd-proteger-vos-donnees-sensibles/