Application security:
Anticipate the threat to reduce costs and guarantee business agility

73% of security incidents concern a web or mobile application[1].

How safe is your corporate data? Hackers have numerous techniques for accessing company data. The skills, resources and determination of today's cybercriminals are almost unlimited. So, what is their most common method of attack? Our research reveals that hackers are most likely to exploit the vulnerabilities of your applications.

The number of successful attacks is constantly growing

Until recently, most companies believed that their data and infrastructure security procedures were sufficient to protect their business applications.

But that's no longer the case. To transform and innovate, enterprises are developing new applications at a frenetic pace, and this is making them increasingly vulnerable to cyber-attacks. Organizations need to be more proactive and anticipate where hackers might target their organization.

Only 20% of companies' security budget is dedicated to the application layer.

The open source software (OSS) that organizations rely on to develop their applications both accelerates their speed to market and significantly increases the quantity of applications released worldwide. However, to maintain this momentum organizations must, in parallel, redouble their efforts to address a number of risks that are inherent in this software:

- Security risks (when OSS contains published vulnerabilities that expose the company to wide-scale breaches);
- Legal risks (when open source license stipulations are not observed);
- Operational risks (when the open source community does not manage or no longer improves the product).

67% of open source software rolled out contains security vulnerabilities[2].

With the massive rollout of open source software, everyone has access to the code, but no one audits it...

Protecting applications quickly and effectively has therefore become a priority. Without an automatic indexing process in place to monitor the use of software, companies typically resort to manual checks that make assessment difficult and increase the risk of errors. In this context, they quickly lose control of their open source components and have difficulty managing them within the framework of the software development process.

Chief Information Security Officers (CISOs) must therefore put in place proactive measures to defend their applications against security breaches, guarantee their legal compliance, and eliminate operational risks.

Security is never complete and must be constantly developed, tested, checked and adapted.

To meet this need for a constant, proactive approach, more automated options are being developed specific to application security, referred to as AST (Application Security Testing). These new solutions combine dynamic and static security testing technologies with in-depth expertise in software testing. They provide optimal protection and enable targeted companies to consolidate any potential breach and contain threats before they can damage their reputation or turnover.

More than a third of consumers are prepared to pay for strengthened security.[3].

1 2017 - Source: Akamai. ** Equifax Hacking (143 million stolen identities)

2 From Black Duck Software code audits realized during merge & acquisitions in 2015

3 Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

Dispelling the myths surrounding application security

Security is no longer the sole preserve of a company's technology teams, but now concerns the wider business as well. To differentiate in the market and optimize application security, it is vital to incorporate best practice company wide. Yet this is not always what happens. When it comes to securing applications, there are several received ideas – let's call them myths – in circulation that lead companies into a dead-end on security due to a misconception that costs and deadlines will be excessive. The following provides an overview of some of the application security myths.

Myth #1:

Internal development teams are in control of security and produce applications that are already secure

69% of applications are open to data theft [4].

Designing applications that are inherently secure is not a foregone conclusion, even for the most seasoned developers. IT development and security are two relatively separate worlds: the vast majority of developers are not trained in security and are often unaware of the breaches in their applications.

1 website out of 8 has at least one critical vulnerability[5].

Myth #2:

Making an application secure slows down go-to-market time and does not meet business flexibility needs

7.2 million dollars[6]. The average cost of a successful attack on a large company's data.

The budget allocated to application security during the development phase is often insufficient. This explains why breaches are systematically detected only when applications are tested at the end of the development cycle. This leaves teams with no choice: to avoid rolling out a vulnerable application, they must delay its market launch. This creates the impression of a certain rigidity in procedures in order to make applications secure.

The solution is to build in maximum security from the start of development, which would enable significant savings in terms of time and resources.

4 2017 - Source: Akamai. **Equifax Hacking (143 million stolen identities)

5 Source: Sogeti ESEC

6 Source: NIST

80 days to detect a breach, 4 months or more to resolve it[7].

An "after the fact" approach may also be dangerous from the perspective of the company's reputation. Once the application is online, its users rightfully expect it to be 100% secure. A security breach discovered too late may seriously damage the company's image and impair the application's usefulness.

For example, 74% of those surveyed would leave their bank or insurance company if a data breach occurred[8].

Myth #3:

Testing an application's security is a long and complicated process

Performing tests downstream, once the application's development is completed, is far from sufficient and does not yield satisfactory software quality results. Thus, it is essential both to introduce security from the outset and to test the solution gradually throughout its development. This makes any corrective action much faster to undertake. By combining automated processes and human expertise in effective and relevant solutions, it is possible to detect breaches by revealing a very low number of false positives. Instead of slowing down an application's development, this approach saves time and money.

7 Source: NIST

8 Source: Capgemini's Digital Transformation Institute Cybersecurity and Privacy Survey

The benefits of AST (Application Security Testing)

> *In terms of security testing, companies need an on-demand service."*
>
> **- Yves Le Floch,**
> Cybersecurity Development Director, Sogeti

Application Security Testing enables companies to make their application security systematic. On-demand services do not require any prior investment, expertise, or specific level of technical sophistication. On a dedicated, secure portal, customers upload their source code or provide the URL of the application they wish to protect. They then have:

- A concise overview of the application's security status;
- The possibility of accessing and starting tests 'on demand';
- Access to different summary reports, explanatory pages on the vulnerabilities identified and how to correct them, and instructions for prioritizing patches.

Some interfaces are collaborative and can help development teams monitor results.

A good on-demand application security testing service enables the elimination of more than 99% of false positives generated by the testing tools.

Protecting applications throughout their lifecycle

Applications abound in all companies in today's digital workplace. Their development cycle is short, with frequent updates – monthly, weekly or even daily. However, each new version carries the risk of introducing new application breaches. Hence the increased need to audit applications regularly across the board.

Reducing the attack surface

Audits enable application breaches to be precisely located, weaknesses to be effectively targeted and the surface open to potential attacks to be reduced. Companies with the most effective protection have typically opted to roll out application security testing. All the applications and their updates are tested rigorously. The method can be implemented in-house and/or in collaboration with a service provider with industrial capacity and the expertise required.

By monitoring applications continuously, identifying threats and protecting itself against malicious acts, an organization considerably limits the opportunities for hackers to attack.

> *When the developer is quickly alerted to a breach, work can immediately begin on the line of code to understand the error and ensure it is not repeated, thereby improving both the cybersecurity and code quality."*
>
> **- Jean-Alain Julie,**
> Application Security Testing Expert, Sogeti

Testing from the outset to avoid wasting time

The earlier security tests are carried out, for example when adopting or developing the application, the more effective the process to correct vulnerabilities becomes. Partly automated, these tests can be performed:

- on the code, source or executable (static tests).
- or on the application in operation (dynamic tests).

However, as soon as the project is about to go live, strengthening the application's security involves going back up the whole development chain to correct breaches, which considerably extends deployment times.

AST as an important brick in GDPR compliance

In May 2018, the General Data Protection Regulation (GDPR) comes into effect. This new European regulation will strengthen controls over the way in which companies and authorities process personal data and its security. These different obligations require that organizations adopt a resolutely cyber-resilient approach, and therefore place security at the heart of their data processing, particularly in application layers.

71% of banking organizations do not yet have a suitable security strategy or clear and specific policies on data protection[9].

Applications and data breaches – some statistics

- 120% new security breaches discovered each year;
- More than 500 million identities, including personal data, are exposed following attacks each year;
- 98% of companies embed open source code (often without knowing it) and 90% of breaches on open source components can be easily exploited.

Strengthening the company and its customers' trust in applications

All companies fear the consequences of either the press or social media channels revealing that they have been victim of a cyber security attack.

On the other hand, providing transparent communication about risk control (carrying out tests and absence of breaches) is an excellent marketing ploy, and could even provide a competitive advantage for both business-to-business and business-to-consumer enterprises.

9 Source: Capgemini - The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure

Application security: client case studies

British Gas uses HPE Fortify on Demand

Sogeti teamed up with HPE (Hewlett Packard Enterprise) to develop Fortify on Demand, a series of on-demand security tests. This service improves applications' security, reduces their cost and increases their efficiency.

The HPE Fortify on Demand solution was chosen for the static and dynamic audit of the code developed in-house by British Gas. The Group had many years of experience in traditional information security, but this had become insufficient. The service developed by Sogeti and HPE enabled British Gas to ensure the compliance of its applications with regulations in the sector.

Furthermore, the company accrued benefits in its application development process, as Paul Phillips, Software Assurance and Integration Director at British Gas explains:

> *"We adopted a shift left culture and now bring the code to maturity more quickly: it is easier to maintain and has fewer vulnerabilities. The volume and severity of these vulnerabilities are considerably lower than when we started to use Fortify on Demand."*
>
> **- Paul Phillips,**
> Software Assurance and Integration Director at British Gas

A major French bank uses AST

How do we enable financial institutions to remain secure and trustworthy?

We helped a banking institution put in place a program for the joint design of innovative applications with its clients and Fintechs. As part of this collaboration, it was essential for the bank to guarantee the security of the solutions rolled out. It opted for a proactive approach and placed security at the heart of application development.

With Sogeti's AST solution, the bank was able to perform fundamental security checks simply and rapidly: assessment of the source code, binaries and the application running or under development. The system found vulnerabilities on three levels of the mobile applications: client, server and network. This made it possible to carry out appropriate security tests on mobile applications to cover all the risk levels, on both internal and external applications, whether live or not.

Avantages :

- Quick and simple start-up;
  - no need for additional hardware or infrastructure.
  - flexible solution based on needs.
- A unique portal accessible from anywhere (the teams are based in Singapore, Switzerland and Paris);
- Rapid results.

These new application services have been operational within the bank since December 2016 and their security is continually reinforced.

AXA Luxembourg talks about its AST project

We were looking for an efficient solution enabling us to integrate security tests in our development cycle.

"We need rapid detection/ reporting readability for our agile development model and we found this perfectly in the Fortify on Demand offer from Sogeti.

"Furthermore, Sogeti's skilled consultants, who are experts in security testing, greatly facilitated the dialog between our security team and our developers.

"We have incorporated the approach proposed by Sogeti in our processes, and we will continue on this track."

- Michael Frippiat,
CISO , AXA Luxembourg

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2016 global revenues of EUR 12.5 billion.

Visit us at:

www.capgemini.com

For more information, contact:

Yves Le Floch
Vice President, Commercial Director cybersecurity France
Sogeti Cybersecurity
yves.le-floch@sogeti.com
+33 (0)1 55 00 13 41

Vincent Laurens
Cybersecurity Practice Executive | Vice President
Sogeti Luxembourg
vincent.laurens@sogeti.lu
+352 31 44 01 276

Jean-Alain JULIE
Application Security Testing Corporate Business Developer
Sogeti Cybersecurity
jean-alain.julie@sogeti.com
+33 1 55 00 12 10

People matter, results count.