APPCHECK NG
ACCURACY IS EVERYTHING

E: info@appcheck-ng
W: appcheck-ng.com
T: 0113 887 8380

Will Web apps security be your GDPR Weakness?

The GDPR Regulations are coming and will be legally executed from the 25th May for us all. What does this mean to you? Well the fines are likely to be penal with the ICO able to fine you 4% of your annual Turnover or 20 Million Euro whichever is the higher.

Whilst these fines will hurt that will be NOTHING in comparison to the reputational damage your business will incur with its customers/partners/suppliers/employees when said breach becomes public. You only have to look at a recent example of a high-profile telecoms company to see what this means: 25% of their customers walked away within 1 year; they lost 62% of their share value in 3 months; ultimately the CEO lost her job a year to the day of the breach.

Could This Happen to you? Well if you have WEB Apps in your business it could. Consider all those people, partners, 3rd parties who have been busily building your apps for the web-how many of them have spared much of a thought for your OR more importantly all those EU Citizens whose data you hold, security? One breach is all it takes to overturn all that Good will built up. Can you afford that?

In this white paper we highlight some of the common issues we've seen over the last year through our research and using the Verizon report to back this up with statistics.

External attacks are the most likely

"While this goes against InfoSec folklore, the story the data consistently tells is that, when it comes to data disclosure, the attacker is not coming from inside the house. And let's face it, no matter how big your house may be there are more folks outside it than there are inside it." - Verizon 2016 Data Breach Investigations Report

More than 75% of attacks are from external sources rather than your internal disenfranchised employees.

Will Web apps security be your GDPR Weakness?

My firewall protects me, so I don’t need any testing

Is this you? Many organisations feel they are protected by their firewall or other forms of external ‘wrapper like’ defence. The fact is that no matter what defences you have in place you will not be un-hackable (the Dark Web Specialist Darkbeam believes that more than 98% of business have already been hacked-they just aren’t aware of it yet). And the landscape is changing every day making it impossible to be ahead of the game, to **say that having a firewall will protect you unfortunately just isn’t the case**. Blue chip companies will spend millions on firewalls but still have data breaches.

What about your GDPR Vulnerability, fines and reputational damage?

In the context of GDPR it becomes ever more critical that the more proactive you can be around security the better. Having **a truly defensible position** and proving you have everything in place will make a difference with your local Regulator.

SQL Injection still the number one vulnerability!

“Injection and serialisation vulnerabilities are the most common types of vulnerability found in web applications. They are often easily over looked even by seasoned developers and are often easily exploited to gain access to databases, remote code execution or command execution. Usually one means all three, depending on how a system in configured it’s usually a short stop from there to completely compromise a system.”
– Graham Bacon, Head of Development, AppCheck.

Web application vulnerabilities are not new and come in many forms, strange then that still at No.1 on the OWASP top ten in 2017 for the number of successful breaches is SQL injection. Last year alone in the UK there were 571 confirmed data breaches through web applications. It is a problem that is not going away, and the trends suggest that it may get worse.

So, considering the stats and the sheer number of data breaches through web applications this is clearly a major threat for GDPR compliance. With the ever-changing threat around web applications new vulnerabilities are always getting discovered and changes constantly being made to applications make this an expanding, complex problem to solve.

GDPR INSTITUT

Will Web apps security be your GDPR Weakness?

Don’t get Equifax’d

The Equifax data breach – this was high profile especially given the nature of their business, **14.5 million users** were compromised through a **web application vulnerability**.

In Equifax’ case they were **doing the checks but missed the vulnerability**. Their vulnerability was discovered in March but not exploited until May and highlights that running regular tests is crucial in staying on top of your vulnerabilities. Perhaps more importantly is understanding the reports and then acting on them in order to gain the coverage your organisation needs.

What are the repercussions, the biggest one is **Reputational damage**, given the nature of what Equifax do this is likely to affect the organisation long term? If you look at the fact that key shareholders sold shares before the breach was disclosed there were clearly fears within the company. Alongside this there will be significant fines associated with the breach which are still to be determined.

Conclusion

GDPR is a massive piece of legislation with multiple areas to consider and there is no quick fix, it will be about you as a company becoming more proactive around securing your data. We know at AppCheck that regular testing will play a part, but it is about you as an organisation prioritising and choosing where to start. The reason we have partnered with the GDPR institute is to make people aware that web app security could affect your GDPR compliance.

References
- Verizon 2016 Data Breach Investigations Report
- Verizon 2017 Data Breach Investigations Report • The Telegraph, Cara Mcgoogan, Equifax hackers targeted 15.2 million UK records, http://www.telegraph.co.uk/technology/2017/10/10/equifax-hackers-targeted-152-million-uk-records/

GDPR INSTITUT

For more information please contact us on:

T. 0113 887 8380

E. info@appcheck-ng.com

W. appcheck-ng.com