mattclarkecto.com // just technology

White Paper

Why Web Developers Can’t Do Cybersecurity

With Cybersecurity becoming an increasing threat to Organisations and Governments, it’s important to bring in specialist skills to protect your digital assets

November 2016

mattclarkecto.com

cto bytes

thecto podcast

I’m still a web developer at heart regardless of the management meetings I seem to spend most of my life in. There’s nothing better for me than getting emerged in a solution for one of our clients, whether it be an architecture problem or dealing with the best approaches to ensure we are using the very latest technology. But within the last two years there has been a very dark cloud over our industry which is threatening both the solutions we are building and our clients integrity.

Cybersecurity is now a very real threat and something that needs to be at the forefront of all of our minds. But how far are away are we from really taking this threat seriously?

Well the situation is really quite bleak because the average web developer, solution designer or architect is a million miles away from being equipped to deal with the challenges (sorry guys) of cybersecurity. In fact many of the average web project developments have no one taking this into consideration, yet the expectation is that it is being taken care of. The reality is we have all gone on holiday and left the back door open!

Why?

7 years ago I was fortunate to get involved in something very secret underground, for a very short amount of time, however it was an eye opener to say the least. It was an eye opener because we have all become so trusting of the tools we use, we all stand on the shoulders of other people’s work and we all assume things are safe and protected. 7 years ago I learn’t the vulnerability of all software and hardware and more importantly the vulnerability of people assuming things are being taken care of. The reality is they are <u>not</u> and they need to be specifically called out on every project and built into every programme.

So why aren’t we doing this? Number one reason is know how, number two reason is cost, number three reason is that nobody assumes their website, e-commerce site or company data is important enough to draw the attention of Mr Robot!! However the reality could not be further from the truth.

Lets deal with each of these points.

Know how, the assumption is your project team is dealing with this. The reality is they are not, why because they don’t understand it all.

Security is a specialist subject and a very wide subject. You can be a vulnerability expert at software but you won’t necessary have the infrastructure, hardware, human vulnerability skills. Each is a discipline in its own right, each as a lot of depth and each needs to be coordinated. Take software alone, it’s not just our software we need to consider, its every item of software that we use to build up the entire system. In fact to take it seriously we need to go right down to the very building blocks of our operating systems and server software.

Cost is a balancing act when it comes to security. The know how becomes expensive and the audit requirements for security are continuous and expensive.

Not to mention the inconvenience to a programme once your security guys start getting involved. What is the right level or balance that must be maintained or what is the minimum level of security?

Are you important enough for someone to hack you? Surely it's governments and high profile targets that hackers are really interested in? This is the line taken by most project teams, however I can tell you over the last 17 years 30% or all the major projects we have been involved in have had some kind of attempt on them. Whether denial of service, state sponsored acts or data breach attempts and these are the ones we have noticed. Take the major ones such as state sponsored attempts, we have had at least one customer that has seen unusual activity from ambitious and competitive countries and I would argue none of the organisations we work for are what I would consider high profile. But the information you gather, the competitive nature of your business has value to others, we therefore cannot assume we are immune.

So what should be our strategy?

How do we put some very simple steps to ensure we are starting to develop a significant cyber security strategy for our digital estate and ensure the *web project* with it's usual pressures for delivery does not open the back door into your organisation and it's data.

1) Proven Security Architecture. When developing your web project architecture, the security architecture must be called out from the start. The security architecture should consider every layer of the application software, developed code, hosting and infrastructure and development operations. It should create a risk assessment for each component of the architecture, provide forensic analysis strategy for each component and deal with the policies, strategies, updates, patches and deployment processes for each layer of the application. The risk assessment will create the master check list for all layers and will ensure that developments, updates and deployments have the correct checks balances and policies applied to them throughout the software life-cycle.

2) Coding and Development Operations guidelines. The security architecture will provide the master plan for security. We then need to interpret this for the web development team. For example what does it mean for coding standards, coding audits, test and deployment procedures? Building this effort into day to day development will minimise the costs and ultimately provide a safer system. However an assurances programme needs to be developed to ensure that ongoing security isn't circumnavigated over time.

3) Assurance and human vulnerability. Assurance is critical to the continued success of your system. The Security architecture will provide the blueprint to the entire security ecosystem. However the architecture must detail particular assurance check points. An assurance check point can be deployed as a tool to test and guarantee we followed a particular standard. This could be an assurance that a test was carried out before a deployment or a code audit took place and penetration testing happened on the right component of software. The assurance concept is a simple check point that holds the entire system to account including the people working in it. Alongside this and alongside our security architecture we need to assess and test, through continuous training and assurance, the human vulnerability of our entire system. This by far, is the weakest link in our security and balances must be sought to ensure we all are aware of the risks. This includes the business and overall decision makers for your project as ultimately this is where risk is not fully understood and assumptions are made that things are happening when they are often not.

4) Data Policy. Data is by far the biggest attraction for any potential hacker. The security architecture will deal with this but dedicated policies must be developed for the storage of data, the transportation of data and overall data life cycle.

5) **Infrastructure Policy.** Again this will be part of the overall security architecture, however a dedicated area must be devoted to the infrastructure to ensure that it meets the architectural requirements. Infrastructure can be a major vulnerability and the audit and risk management of your infrastructure needs particular attention.

6) **Compliance.** Where possible organisations should reach for international standards and compliance. Over the years I have seen many organisation dodge compliance because of the cost and pressure it can put on your organisation. PCI compliance being such an example, however these standards have been created for a reason? I find it very strange that organisations and project teams look to dodge them. Ensure they are part of your security strategy.

6) **Accountability** is my final recommendation. At the start of this paper I talked about the assumption that security is being taken care of. Accountability must rest with someone to ensure the security architecture and its assurances and being maintained at every stage of the software life-cycle. It is critical that one named individual knows they have this responsibility and are being paid to provide the necessary service.

But what do we do about projects inflight or systems that have been running for some time?

It's not too late. The above steps can be deployed to any project at anytime during its life-cycle. The security architecture can be developed as part of a simple security audit which will provide a set of recommendations to get you on the road. Equally the same approach can be used to keep your security practices up to date.

> "My key recommendation is to ensure security and a security strategy appears as a line item in all project planning"

For more information or if you require any advice on web project security please contact me at matt@mbclarke.com

About the author

Matt Clarke is Chief Technology Officer at a leading UK based digital technology agency. He advises CTOs, CIOs, CMOs and boards on technology and has been responsible for numerous high profile projects across E-Commerce, The Enterprise Digital Estate, IoT, Cloud, Mobile and Big Data.

For more information please go to;-
https://mattclarkecto.com/mywork

For more white papers go to;-
https://mattclarkecto.com/white-papers/