Secure Application Services – A Practical Viewpoint

When tech investor Marc Andreessen suggested in 2011 that "software is eating the world"[1] he recognised that software applications help businesses grow faster. And he was right.

The digital transformation that most businesses have embarked upon relies on the ability and the agility to use software to increase operational efficiency or launch new products and services.

However the demand for first mover advantage has placed immense pressure on developers who are being asked to get their applications out to market as quickly as possible. This, combined with a lack of investment in developer security training, can often mean that applications are released with vulnerable code. Gartner figures show that nearly **80 percent** of applications written for the web contain at least one vulnerability on initial assessment[2] – a vulnerability that could lead to a significant security incident. If applications make such a difference to business performance, application security should be a priority for every organisation that wishes to avoid the availability, reputational and cost pitfalls associated with flaws in application code.

Digital transformation demands an agile approach to application security

With digital transformation gathering pace, security needs to be part of an iterative design and testing process, rather than uncovering risks just as an application is ready to go – or worse, already in production. After all, time is also money and The National Institute of Standards and Technology has reported that it is 30 times more expensive to fix vulnerabilities in post-production than at the design, requirement identification and architecture stage.[4]

Digital transformation will usually also require security program transformation to ensure security practices evolve as your applications, application delivery and application estate evolves. It is a great opportunity to embrace new technology and practices and be more secure.

WhiteHat Industry Blog[3]

Figure 1 Top categories for attacks. NTT Group Global Threat Intelligence Report 2017

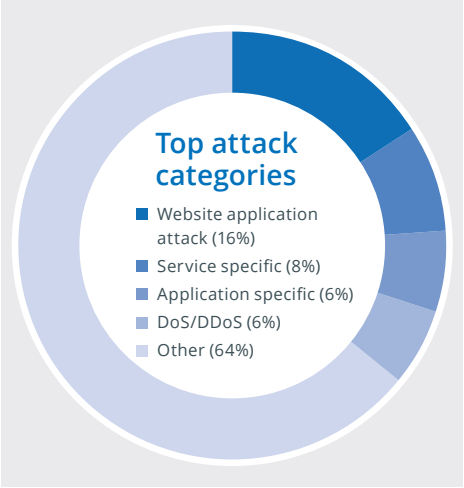
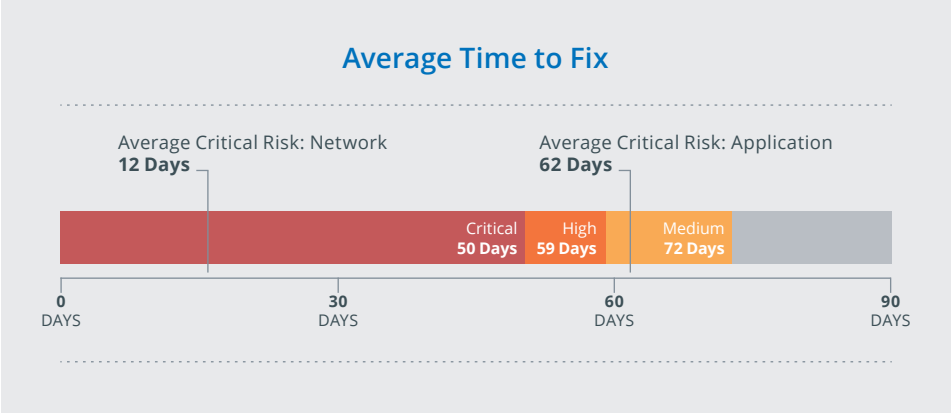


Figure 2 On average, it takes approximately 62 days to fix a critical risk to an application. Source: Edgescan



1. Essay: Why Software Is Eating The World, Marc Andreessen 2. Gartner: Forecast Analysis: Enterprise Application Software, Worldwide, 2Q15 Update
3. WhiteHat Industry Blog: Digital Transformation = Application Security Program Transformation 4. Veracode press release

Copyright© NTT Security 2017

The challenges of application security maturity

The 2016 SANS Institute State of Application Security survey highlighted a host of issues in security-related processes and skills – saying "it takes a village to protect applications" – made up of a complex and often siloed ecosystem of security staff, developers, business units, architects and quality assurance teams. The lack of clear, consistent accountability for security-focused best practices as new applications are developed and go to market, means that security is often overlooked or implemented far too late in the development lifecycle process. We talk to many organisations that want to bring a halt to the adversarial trade-off between speed-to-market and secure applications, by building security into the software development lifecycle (SDLC). However, the SANS report concludes that application security remains at an early stage of maturity, and that it will require the right focus and sufficient resources to grow – resources which are in short supply.

How mature is your application security?

Issue	Challenge	Answer	Requirement	Maturity Level
Visibility	Do you have visibility into your application vulnerabilities and threats?	No	Application assessment based on security testing and analysis	LOW
		Yes	Goal-orientated or threat-based testing	HIGH
Breadth vs Depth	Do you assess the breadth and types of application vulnerabilities, to understand your security posture?	No	Vulnerability and application assessment to provide a full list of known vulnerabilities	LOW
		Yes	Pen Testing to exploit known vulnerabilities	HIGH
Risk Prioritisation	Do you understand the priority of your application vulnerabilities or threats?	No	Vulnerability scanning and risk analysis to rank and prioritise application vulnerabilities	LOW
		Yes	Pen testing to explore known vulnerabilities for true risk and impact identification	HIGH
Agility	Do you have an integrated and cyclical security testing process to work alongside your SDLC?	No	Adaptive security testing framework during the SDLC	LOW
		Yes	End of SDLC validation of security testing	HIGH
Assurance	Do you address application vulnerabilities with the right mitigation techniques?	No	Early implementation of the correct security controls into the SDLC	LOW
		Yes	Validation of existing security controls and suggestions for further enhancement	HIGH

And even where there are clear lines of responsibility, application security must constantly adapt to what business users and customers expect. Critical web applications often used to be secured by perimeter firewalls, but the transformation in the way web apps are delivered means that this is no longer effective. As users consume applications on an ever-growing array of devices such as mobiles and tablets, accessing an organisation's most valuable data beyond the perimeter and into the cloud, the security perimeter has shifted too. And then there is the proliferation of elements such as APIs, micro-services and containers that need to be designed and deployed and have served to further increase the scale and complexity of an application's potential attack surface.

Gartner believes that, by 2019, most mainstream development frameworks will have incorporated automated security vulnerability and application security testing.[5] However, whatever benefits are introduced by security-aware development frameworks will take time to propagate to the vast majority of production web applications. This leaves organisations needing a way to continuously manage the risk of today's attackers accessing, stealing or tampering with sensitive data accessible through internal or external applications, via vulnerabilities such as SQL injection, cross-site request forgery (CSRF) and XSS. And then there are the new application delivery models to consider. What about DevOps and Platform as a service (PaaS) – not to mention technologies such as mobile application programming languages and frameworks, and rich internet applications? Even if application security teams have long-term aspirations to do things differently, many have little choice but to use tactical penetration testing, on applications already released into production, to uncover issues before attackers do.

5. Gartner Report: How to Seamlessly Integrate Security Into DevOps

Copyright© NTT Security 2017

A new approach to application security

One way to increased application security maturity is to move away from an in-house, DIY approach and instead make use of third-party specialist application security service providers with the knowledge, skills and resources gained by working daily with a wide range of customers. To help organisations identify and remediate web application risk today, NTT Security has combined elements of application testing and consulting into a set of complementary services – designed to help organisations incrementally improve their security posture. We call this offering Secure Application Services (SAS).

A combination of services including penetration testing, vulnerability assessment, advice on security policies and implementation of security controls such as web application firewalls (WAF) are delivered by experienced web application security specialists. Secure Application Services offer customers a cost-effective solution to both the resourcing and technology challenges of web application security and is applied to deliver maximum impact. Secure Application Services can support you whether your application is production-ready and needs the final validation prior to full release, that only a manual penetration test can provide – or whether you are looking to incrementally assess and remediate vulnerabilities using automated tools, as the application moves through the SDLC process.

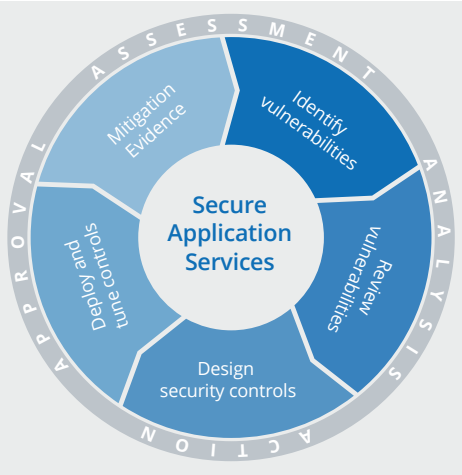
This paper is aimed at information security professionals who want to develop an effective, practical and long-term approach to detecting and mitigating web application security flaws, as well as reducing the resources required to manage potential vulnerabilities in both new and legacy applications. Our aim is to help businesses make it easy to build application security into their release lifecycle by offering scale, speed and efficiency. With each cycle of testing, an organisation will enhance its security posture.

How do Secure Application Services work?

Assessment: identify vulnerabilities

Traditional approaches to testing must evolve in the face of changing threats to your applications, as well as new development techniques. Very few of the organisations we talk to have a comprehensive approach to identifying and remediating application vulnerabilities, particularly when it comes to assessing internally-developed web applications. This is often due to a shortage of resources and many organisations are eager to investigate how to automate the assessment of critical applications – particularly in legacy systems for which the source code is unavailable. We help organisations make their testing budgets work harder and absorb less resource with a combination of manual and automated testing.

Figure 3 Our structured approach to web application security – IWAP helps reduce application risk for your business



Analysis: review findings; create control sets that work for your business

To improve the security of applications, organisations not only need to establish full visibility to vulnerabilities, they must also put the right controls in place – in the knowledge that traditional network security safeguards are insufficient.

To ensure full value and a lasting impact from agile web application security, many of our customers value the perspective of a third party. Our consultants do not just review identified vulnerabilities; they also prioritise them and the required mitigation actions, using their extensive knowledge and experience to design the correct controls.

The key advantage of this approach is the ability to streamline and put into production the design and implementation of security controls – a process which has historically been performed manually and is therefore time-consuming. By providing a structured and sustainable model for the creation of control sets, it is possible to scale up the implementation of security controls, making the process more accurate and cost-effective.

Security professionals should immediately create a plan to mitigate critical vulnerabilities by using technologies like web application firewalls (WAFs) to provide development teams the necessary time to produce the remediation fix.....By performing and reviewing the results against dynamic application security testing on staged applications, security practitioners can help development teams correlate security flaws manifesting in runtime with vulnerable software code. This reduces the number of critical and high-risk vulnerabilities that go out in the first place.

WhiteHat Security:
Web applications maturity security statistics report 2016

Action: implementation of controls

Our approach seeks to not just recommend mitigations for the customer to digest, rather, NTT Security will also implement the correct controls – making use, for example, of the protections offered by a web application firewall (WAF).

Our consultants seamlessly implement the agreed controls to ensure that any vulnerability exposed during the Assessment and Analysis phases is mitigated against in a structured and unobtrusive manner. The goal of the Secure Application Services is not only to address isolated issues, but to transform the underlying maturity of web application security.

Copyright© NTT Security 2017

Approval: making application security business as usual

Once the correct controls are in place, our clients want the evidence that the vulnerabilities have been successfully mitigated against. This clearly demonstrates the value of the service, but also the value of embedding application security into future business as usual development: keeping security teams involved in a continual iterative process that includes planning, designing, coding, and finally – testing.

Benefits of Secure Application Services:

- Reduced attack surface area
- Optimised application security delivery
- Faster go-to-market timelines
- Increased visibility into the application
- Improved compliance
- Secure policy framework for web applications
- Brand confidence

Summary and next steps: building a mature approach to web application security

Data is often referred to as the oil of business. If this is true, then applications are the engine and to maintain availability and reduce risk, their security should be constantly fine-tuned for corporate wellbeing. Just as agile software development sought to deliver code incrementally – in our experience, many organisations need to break down the current approach to web application security by introducing a more iterative process to continuously reduce risk.

With an acute skills shortage, very few organisations have established the right combination of testing and application security controls to sustain a mature, best practice approach. At the same time, many businesses are accelerating their digital transformation. Industry analyst Quocirca recently identified that finance companies typically are maintaining a minimum of 800 mission-critical applications, other organisations 400 – a growing number of which will be connected to the internet.[6] NTT Security's Secure Application Services (SAS) can help application security teams access the skills, processes and technology experience they need to reduce web application risk.

To speak to a member of the application security team about how our Secure Application Services can help you establish the right testing and application security controls for your business, please speak to your NTT account representative or visit: nttsecurity.com for contact information.

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.

6. Quocirca Report: Outsourcing the Problem of Software

Copyright© NTT Security 2017