

CORE IMPACT CUSTOMER SUCCESS STORY

SOLUTION SUMMARY

CUSTOMER TYPE | Local Government for Borough of England, United Kingdom.

CHALLENGE | Improving overall IT security standing and meeting compliance requirements.

SOLUTION | CORE IMPACT Pro, the first comprehensive penetration testing software solution for assessing organizations' most significant IT vulnerabilities and information security threats.

THE COMPANY

Royal Borough of Windsor and Maidenhead



The Royal Borough of Windsor and Maidenhead is a region of Berkshire, United Kingdom, located just west of London in South East England. With a population of over 140,000 citizens, located just a short trip from the city, the region is known both as popular place to live and as a destination for tourists who visit in search of well-known attractions including Windsor Castle.

As with any contemporary government entity, the Borough maintains sizeable IT operations including many public-facing Web sites that offer online services to the region's inhabitants and government employees.

Windsor-Maidenhead's Security Architect leads a team responsible for overseeing all of the Borough's IT operations, in addition to preparing for security audits required by the U.K. government and industry groups including the Payment Card Industry (PCI). He also spearheads procurement of Windsor-Maidenhead's IT security and vulnerability management solutions.

"One of the biggest advantages of adopting CORE IMPACT Pro is that for a fixed amount of money we are now able to perform a far wider spectrum of testing across the entire Borough; If I had to do everything via third parties and consultants we simply wouldn't be able to test as broadly as we do today based on the budget that we have to work with."

THE CHALLENGE

As with most government entities worldwide Windsor-Maidenhead has added considerable breadth and complexity to its IT systems over the last decade, in particular as it has moved to make many of its public services available to its citizens via Web applications.

Through those efforts, Windsor-Maidenhead now supports a number of online transactional systems that allow citizens to pay bills and register for services over the Web, requiring the government to securely handle payment cards and customer account data on many of its sites.

As a result, the Windsor-Maidenhead government has also found itself in possession of a rapidly growing stockpile of electronic records, many of which contain the sensitive personal information of the regions' tens of thousands of citizens and employees.

Based on those needs, the Borough's IT security team has embraced the process of automated penetration testing as a method of assessing vulnerabilities and targeting its operational security efforts to address critical risks, and to remain compliant with regulations including the U.K. government's Code of Connection and the PCI Data Security Standard.

"We've been trying to improve IT security across the board within our local environment for some time, and we also have to consider these increasingly stringent mandates that we face both from the U.K. government and in the form of PCI," said the Windsor-Maidenhead Security Architect. "With these regulations requiring more frequent vulnerability assessment and Web applications testing, we wanted to create a penetration testing program that would help us both meet external requirements and assess IT systems and applications in-house before they ever go live."

THE SOLUTION

To help the Windsor-Maidenhead government rapidly advance its IT security standing and comply with audits, the Security Architect and his team decided to formalize what had previously existed as a part-time penetration testing program.

As a major element of this process, the team sought a more polished, commercial-grade penetration testing solution to replace the free, open source tools that it had traditionally used to carry out security assessments. The Windsor-Maidenhead team also desired a

pen testing product that would dovetail with the Borough's existing vulnerability scanning tools, notably, Tenable Network Security's Nessus scanner and Landguard's GFI software, along with the Borough's internal patch management systems.

After surveying the available products, Windsor-Maidenhead decided that CORE IMPACT Pro's combination of automation and commercial-grade exploits made it the best choice for expanding its testing program.

In addition to helping the Borough meet specific compliance requirements, the Security Architect said that his staff has used IMPACT Pro to embed the penetration testing process throughout its IT programs and foster improved security in many other ways. On top of testing its systems on a quarterly basis, the Windsor-Maidenhead team now also performs tests after any major "perimeter" configuration changes, and prior to the roll-out of any new Web applications.

Another benefit of using IMPACT Pro is that it has allowed the government agency to mature its program rapidly without adding new, dedicated testing staffers.

"We've previously used open source tools for vulnerability assessment but the level of automation in IMPACT Pro, the ability to discover hosts and assess services, and the availability of so many exploits for each system, has made it a whole new ballgame for us," he said. "Using IMPACT as a basis we've developed a structured approach to security testing that's become part of our normal security operations and we're able to run a lot of tests with only a few dedicated workers."

"If you look at the reports that you get from running tests using IMPACT, every vulnerability is prioritized; this allows you the ability, within a relatively short timeframe, to define your biggest risks and generate the same types of assessment data internally that you'd typically get from third party consultants; it definitely made us more aware of the state of our operations, and increased our ability to maintain controls."

THE RESULT

Easing Regulatory Compliance

One of the primary reasons that Windsor-Maidenhead sought to adopt automated penetration testing was to maintain compliance with both U.K. government requirements and the PCI Data Security Standard between consulting engagements, and to ease preparation for voluntary and required third-party audits.

In addition to meeting the prerequisites of PCI DSS Requirement 11.3 which dictates that organizations perform penetration testing at least once a year and after any significant network upgrade or modification, the Security Architect said IMPACT Pro helped prepare for many other elements of the audit process, such as proving the efficacy of other mandated security controls.

"Based on these regulations we now have to do self-assessment for internal networks and generate reports that show that we're maintaining the right controls within systems," he said. "IMPACT Pro has helped us identify vulnerabilities that we had on our perimeter and close gaps prior to external pen tests, making it easier for us to both prepare for and undergo the audit process."

Securing Web Applications

The rise of Web applications has added layers of complexity to the IT ecosystem, forcing security professionals to quickly get up to speed on a constantly changing array of programming formats and potential vulnerabilities. By running IMPACT Pro across its Web applications, many of which handle sensitive personal data or card information, Windsor-Maidenhead has been able to identify and eliminate flaws that otherwise might have exposed its systems to potential attacks or compliance problems.

"We've managed to identify some low hanging fruit in our Web applications, including cross-site scripting and SQL injection issues," said the security team leader. "This has allowed us to both fix anything that was developed in-house and to identify any problems introduced by third-party developers, who have typically been able to provide fixes for their code. Testing web apps is much different than testing a network, but IMPACT has given us the ability to carry out this work without introducing a steep learning curve."

Maximizing Internal Resources

With a relatively small IT security team responsible for securing a wide range of assets, the Borough needed a penetration testing solution that could be used by its existing staffers without requiring significant upfront training. By adding IMPACT Pro to its vulnerability management programs, the government agency has been able to ramp up testing without being forced to hire additional workers.

"I traditionally ran a lot of the pen tests myself because we have only a small number of staffers directly responsible for this area of security, but the idea was to bring something in that would make it more of a departmental effort," he said. "When it comes to patching the network or changing an application configuration we typically hand off to someone else, but, you still need to inform them what to do."