



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best Security Company'

BlackBerry Security Assessment

BlackBerry® is a sophisticated messaging solution designed to enable mobile employees to wirelessly connect with corporate resources anywhere in the world as long as they are within range of a standard GSM/GPRS network. This mobile messaging solution offers remote email and Intranet access, along with standard mobile telephony functionality, and is designed to bridge the standard corporate network perimeter; therefore requiring special security consideration.

The NGSConsulting BlackBerry Security Assessment service is specifically designed to identify configuration and deployment flaws associated with integrating the mobile solution into a corporate environment, and provide detailed remediation advice.

The BlackBerry Security Assessment makes use of a focused and proven methodology to identify security flaws unique to BlackBerry (in all permutations of possible deployments). NGSSoftware's consultants assess the architecture and configuration of the BlackBerry hosting environment, evaluating both legitimate and illegitimate points of access, and enumerate any potential security vulnerabilities or departures from best practice.

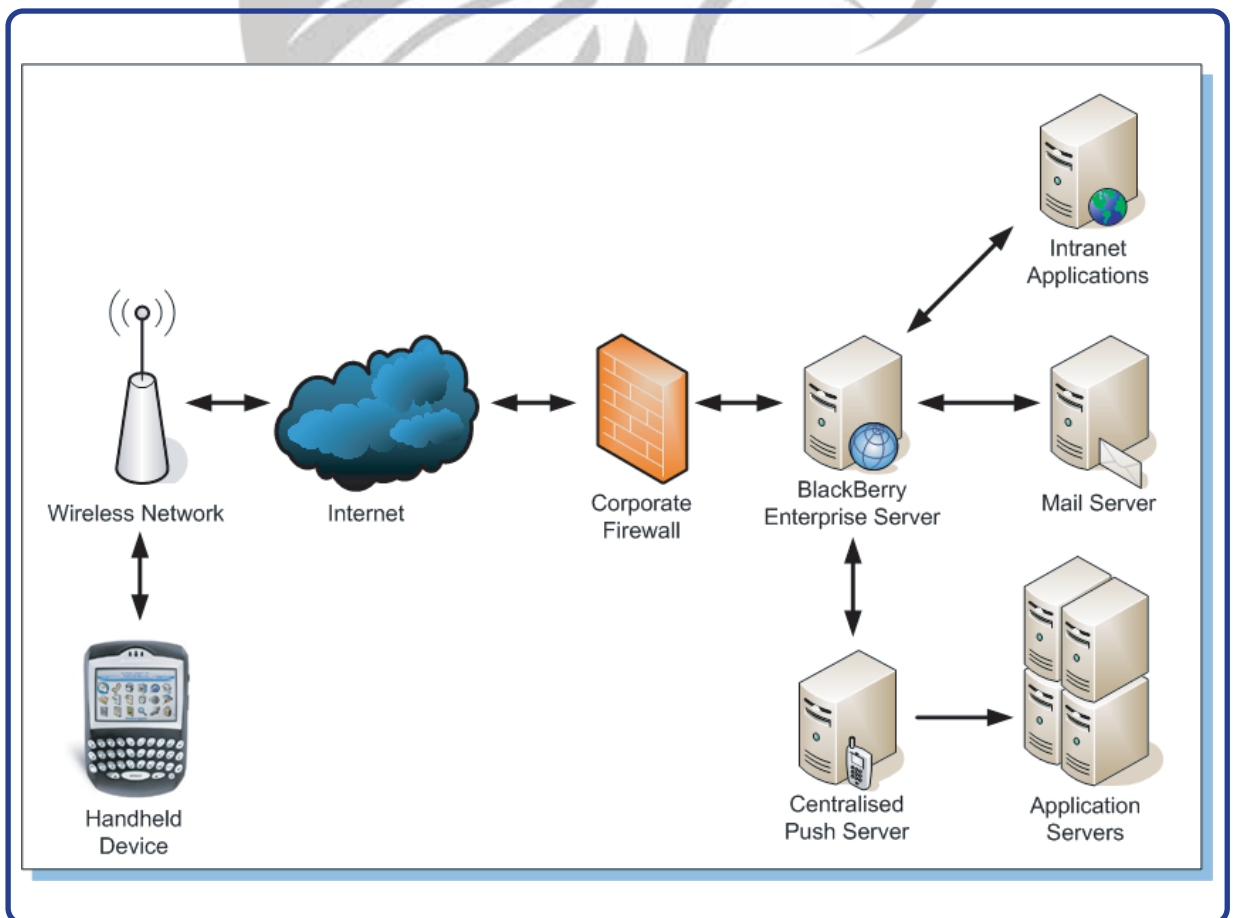
Examination of the hosting environment from a remote perspective is also conducted. Here, consultants explore access restrictions and probabilities of vulnerability exploitation from a mobile BlackBerry handheld device, along with the BlackBerry Desktop integration software and other related Internet-bound connection technologies.

This special NGSConsulting security assessment process allows our clients to evaluate the likelihood of potential attack, enabling them to secure their BlackBerry infrastructure.

The detailed technical and management reports provided by NGSConsulting allows client organisations to objectively assess the security of this mobile messaging platform.

As well as exposing risks during the BlackBerry Security Assessment process, NGSConsulting helps to equip clients with the information necessary to remedy any security vulnerabilities through both detailed technical explanations and skills transfer activities.

The application of our world-leading technical security skills - combined with our research and development facilities - has helped ensure that our services to the world's top commercial organisations and vital government agencies are second to none.



BlackBerry
Security
Assessment



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

BlackBerry
Security
Assessment

BlackBerry Security Assessment

» Methodology

The BlackBerry Security Assessment methodology is broken into a number of distinct security phases to ensure that all aspects of the deployment are covered and no potential vector for future attack is left unexamined. Phases include:

- » **Project Initiation** - During this phase NGSSoftware's Consultants liaise with the client to determine the scope, limitations and timescales of the project. This ensures that from the inception of an engagement the client is fully informed as to what will and will not occur during the assessment.
- » **Assessment of the corporate BlackBerry infrastructure components** - This phase focuses upon the discovery of hosting related security issues and vulnerabilities such as base operating system hardening, patching levels, default installation settings and access controls. During this phase of the assessment process consultants will develop a detailed overview of the infrastructure, potential security vulnerabilities, and threat levels.
- » **Assessment of the BlackBerry integration with corporate application servers** - In this phase, consultants review the levels of access control and data segregation between critical components such as the BlackBerry Enterprise Server installation, corporate Mail services and Intranet web services. This is followed by a similar review of the BlackBerry Push Server's integration with other corporate application servers.
- » **Audit of the BlackBerry Enterprise Server configuration policies** - Consultants review the BlackBerry specific policies responsible for managing connections to auxiliary corporate application servers, BlackBerry desktop agents, and roaming BlackBerry handheld devices. Care is taken to ensure that BlackBerry deployment policies mirror established corporate security policies applicable to other mobile computing or messaging devices.
- » **Assessment of BlackBerry Workstation desktop software** - In this phase, consultants review the configuration of the BlackBerry desktop integration and synchronisation software, evaluating the robustness of the solution to prevent malicious or unauthorised data transportation. Focus is also aimed at the confidentiality and integrity of the data during synchronisation and backup procedures.
- » **Audit of Intermediary Segregation Devices** - To integrate BlackBerry technology into an existing corporate environment, additional security changes must be made to firewalls, routers and other network segregation devices. In this phase, consultants will review firewall policies and ACL's to identify any potential failings and provide guidance on optimisation.
- » **BlackBerry Penetration Test** - In this phase NGSSoftware's consultants will use standard BlackBerry handhelds (and related technologies) to access the offered BlackBerry Enterprise Server services and seek to identify security vulnerabilities that could be exploited by either authorised or unauthorised users. In some cases this phase may expand into an application security assessment if a custom multi-tier application is present, and authorised by the client.
- » **Vulnerability Exploitation** - During this phase of an assessment, consultants will work with the clients' technical staff and, in a controlled manner, exploit potential security vulnerabilities in the infrastructure. Additionally, this phase will see consultants' deploying their expert knowledge in defining bespoke vulnerabilities and the establishment of infrastructure security threat exposure.
- » **Recommendations on Findings** - Based upon the review of infrastructures and the exploitation of vulnerabilities, consultants will offer remediation recommendations to the client. These recommendations are based upon the findings of the assessment process, current and future threat levels, and the requirements of the client.
- » **Documentation and Final Reporting** - During this phase, a detailed Final Report is created, containing the various findings and recommendations as a result of the BlackBerry security assessment.

» Benefits

Selecting NGSSoftware as suppliers of BlackBerry security assessment services has a number of key benefits:

- » A BlackBerry Security Assessment from NGSSoftware provides a detailed overview of existing security vulnerabilities within a clients' BlackBerry deployment that could potentially be used in attacks and exploitation. Additionally, as a result of our globally recognised expertise in the field of application vulnerability research, NGSSoftware's Consultants can provide insight into developing threats and as yet undisclosed vulnerabilities.
- » A BlackBerry Security Assessment by NGSSoftware also enables clients to assess their levels of security risk exposure. Consultants can subsequently employ this knowledge to assist clients to secure their infrastructures and mitigate risk. The BlackBerry Security Assessment process assesses the current security infrastructure of clients' existing security safeguards and control mechanisms. This assessment is conducted using a mix of NGSSoftware's proprietary tools, as well as our consultants' expert knowledge and significant depth of experience.



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

BlackBerry
Security
Assessment

BlackBerry Security Assessment

» Deliverables

During the BlackBerry Security Assessment process, NGSSoftware's Consultants are available to discuss any results that may have been formulated, as well as outlining the processes involved.

The key deliverables throughout the assessment consist of:

- » Immediate notification to our clients of any high-risk vulnerabilities as and when they are discovered.
- » Delivery of interim reports detailing testing completed and findings at the end of each working day.
- » Scheduled conferences at the beginning of each day to discuss issues identified in previous daily reporting.
- » Consultants will be available at any point during the assessment process to discuss any issues that may arise.
- » A Final Report encompassing all activities and findings during the course of the assessment. This report is split into several key sections:
 - » A Management Summary listing areas of weakness and their respective business impacts.
 - » An Assessment Overview detailing the scope and objectives of the project undertaken, and the methodology utilised by the Consultants.
 - » Technical Findings detailing any security vulnerabilities discovered during the testing process, and providing detailed explanations of all the security implications. Comprehensive remediation information will be supplied including alternatives should the preferable solution be impractical.
 - » Conclusions detailing managerial and technical recommendations to the client, with a view to mitigating short term risks, as well as long term strategic solutions.
 - » Exploit Code - Where applicable NGSConsulting will provide the unique service of providing clients with demonstration exploit code.
 - » Additional Recommendations - Where the client is unable to patch any affected products, or the costs of doing so is prohibitive, NGSConsulting will provide a range of recommendations to mitigate any vulnerabilities discovered during the testing process.
- » A presentation to technical or management staff follows the delivery of the final report.

» Assessment Offer

If you feel that you are not receiving an adequate service from your existing security supplier, NGSConsulting would like to extend the opportunity of a no cost, no obligation 'mini-audit', provided under an NDA.

This allows our consultants to demonstrate their technical abilities and also allows future clients to assess the strengths and weaknesses of their existing suppliers.

For further details of this offer, contact info@ngsconsulting.com

» Contact Details

Web: www.ngssoftware.com

Support: support@ngssoftware.com

Sales: sales@ngssoftware.com

UK Head Office (London)
Next Generation Security Software Ltd
52 Throwley Way
Sutton
Surrey, SM1 4BF
United Kingdom

Australian Office (Sydney)
Next Generation Security Software Pty Ltd
Level 19, 2 Market Street
Sydney, NSW, 2000
Australia
ABN: 83 119804803
Regional Web: www.ngssoftware.com/au
Regional Sales: australiasales@ngssoftware.com

Tel: +44 (0)208 401 0070
Fax: +44 (0)208 401 0076

Tel: +61 (0) 448 692 022