September 2010

Middleware Risks

Guidance for Security Managers

An MWR InfoSecurity White Paper

MWR INFOSECURITY

Foreword

As a security consultant and researcher I find myself regularly engaged in testing the effectiveness of security controls for some of the world's leading organisations. By performing this role I am ideally positioned to observe the current state of middleware security. What I have seen has led me to the conclusion that this aspect of IT currently represents a gaping hole in the security of the businesses I work with.

In particular with technologies such as IBM WebSphere MQ, the implementations in highly sensitive and business critical environments are often not fit for purpose, which it should be to ensure the effective management and mitigation of information risk. At the present time organisations are not utilising the security controls within these middleware technologies or the components that interact with them. The result is that the World's leading organisations are exposed to excessively high levels of risk due to inadequate or insufficient security controls in technologies that form a critical part of their business.

The observations I have made of these important areas of technology in combination with my conversations with other people engaged in this field has influenced me to write this white paper. It is intended to raise awareness in this area and to stimulate further discussion within the security industry and the wider business community that relies so heavily on these technologies. It is my hope that this will lead to an improvement in the security of these business critical environments.

I welcome your feedback about this white paper and encourage you to contact me directly with comments or ideas about how to move forwards with the issues surrounding Middleware security.

Martyn Ruks
Technical Director
MWR InfoSecurity

Introduction

Middleware is the unheralded workhorse of the Enterprise and has the responsibility for moving data between business applications. It provides a common interface for a wide variety of technologies and application platforms that all need to communicate between each other. It is the technology that actually delivers the orders to your warehouse, the invoices to your finance department and the status reports to your customers.

Message Oriented Middleware (MOM), of which IBM's WebSphere MQ is one example, is where your business data is transferred between different systems in a standardised manner by placing the information within individual messages. This environment can be thought of as the organisation's true communications backbone which is typically used by computer systems and application components rather than individuals. As the perimeter of your network becomes blurred and indistinct this backbone extends out into partners and suppliers which we neither understand nor trust.

It should be appreciated that this type of messaging technology underpins the operation of every large company across the globe.

Whether your customers are transferring money, ordering goods or viewing the status of their flight it is highly likely that the information has been transferred using Messaging Oriented Middleware. In an era where any given transaction is responsible for triggering multiple business processes even the slightest inconsistency in the handling of data in the middleware layer can have severe implications for an organisation.

For a business that uses this type of middleware to work effectively these messages need to reliably reach their destination, the information contained within them needs to remain confidential and messages should not be changed or inserted without proper authorisation.

"Put simply confidentiality, integrity and availability are all highly relevant to the security of the environment and if any one of the business requirements is not met the operational effectiveness and therefore the profitability of the business is at risk."

Most businesses recognise the importance of middleware from a business continuity perspective but not how security can impact on this. In your organisation do you understand how your middleware architecture affects your ability to mitigate its associated risk?

Organisations within the financial sector are heavily reliant on IBM WebSphere MQ and similar technologies for everything from Internet Banking, intra-bank money transfers and lots of other types of transaction. However, in virtually every market sector organisations need to move data reliably and cheaply around their business between their applications.

In your organisation what data flows over your middleware? What are your requirements for ensuring its confidentiality, integrity and availability as well as maintaining accountability for transactions?

The Challenge

Given the importance of middleware to an organisation's success it is critical that it does not expose them to excessive risk. Given the complexity of the environments within which it operates this leads to a number of challenges that organisations must solve for middleware to enhance and not expose their businesses to risk.

At this point it should be noted that in the past I have personally conducted detailed research into the security of IBM's WebSphere MQ which is one of the most widely adopted technologies in this area of IT. Further details about these findings can be found in my technical white paper on the subject[1]. Therefore, this discussion is centred on this product; however, the same threats and risks are associated with any MOM solution.

To be able to secure an environment that includes MOM there are principally two approaches to securing the business processes that rely on it.

- **Protect the confidentiality of messages** containing the sensitive data using encryption and integrity protection (such as message signing)

- **Protect the whole system** from attacks against the underlying platform and its interfaces through the implementation of a secure configuration

In reality the only viable solution for effective risk mitigation is to employ both methods; however, in practice very few organisations enforce all of these controls to the level that is required. The problem with the approach of choosing to do one or neither of the above is that viable attack vectors still remain. From my experience very few organisations have successfully implemented either one or both of these approaches and in the majority of cases attempts to enforce controls within the technology itself are either incorrectly implemented or incomplete.

Therefore, the reality is that many organisations are sitting on a ticking middleware security time bomb. There are many compelling reasons why these time bombs expose so much risk to the organisation which is sitting on them. One challenge is to understand how you can measure this risk and whether there is one within your organisation.

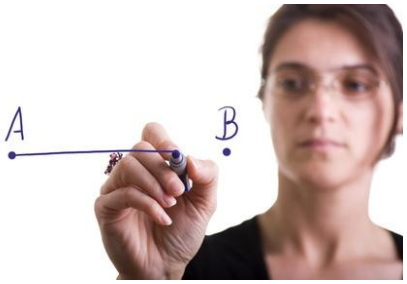
As discussed previously the main reason for this concern is that because of how the technology is used a successful breach could have major significance to the organisation's business, irrespective of the market sector they operate in. In addition, if a breach were to happen the techniques to investigate how it occurred, actions that are required to prevent it happening in the future and to bring those responsible to account aren't widely understood.

Another problem on the horizon for organisations relying on middleware is compliance; the dreaded time when the auditor asks the tough questions about the technology. Up until this point auditors have generally stayed clear of middleware and have chosen to focus their attention on the technologies with widely documented security auditing and testing methodologies associated with them, including web servers and databases.

However, recent security breaches that have involved the theft of data from internal networks have resulted in more and more auditors asking the question "So how does the data get from A to B?"

The confidence in their reply which is often "it's the middleware that does that" is likely to be dented when the auditor then says to them "demonstrate to me that you have secured it". It is also often the case that MOM is responsible for transporting personal or cardholder data and therefore fall within the scope of compliance requirements such as PCI DSS[2]. In these circumstances the auditor should be able to have complete visibility of how you are demonstrating compliance based on the strict requirements of the standard.

The evidence to support the assertion that the auditors are getting their heads around middleware is not easy to find but it does exist.



"If you look at the attendance of the premier messaging technology conference, IMPACT[3], you will observe upward trends in the attendance at the security tracks and you can be confident that auditors are now filling some of those seats."

The stark warnings raised in sessions at events such as IMPACT will surely be heeded by the auditors even if senior management do not because they are either not there to hear them or that they are there and don't understand the implications of the messages they are hearing.

It is also a common assumption that when the day comes to think about reducing the risk associated with middleware there will be a dusty and long forgotten security switch that can simply be thrown to make everything alright. Unfortunately, the reality is that this analogy breaks down if it is believed that setting this switch to "on" solves all the problems. Whilst most organisations are not using them, in general middleware does have security controls built into it.

Nevertheless, these controls are more sophisticated that being "on" and "off" and to use them in a manner that provides effective risk mitigation is not easy in complex business environments. These controls require integration into system design, architecture, network and system infrastructure and into the applications that run within the environment.

Given that these environments need to achieve high availability and are highly integrated into the core of business process, change is not easy to achieve.

The intention is not to paint a picture that no one is employing security controls within their middleware and specifically within technologies such as IBM WebSphere MQ. However, a conclusion can be drawn where organisations are not using security controls in a manner that protects them from all the risks they are exposed to. Whilst some configure and maintain their systems in a manner that offers some protection against some threats they are not doing enough to secure their systems properly. The experience of reviewing, testing and auditing WebSphere MQ installations for large multinational corporations across multiple market sectors shows it to be unquestionably true. The question is what is more scary, those who know the problems and choose not to resolve them, or those who haven't even asked the question yet?

Recommendations

So if your business is relying on Message Oriented Middleware (MOM) what can you do to reduce the risk you might be exposed to?

At this point it is worth noting that it is not the intention of this white paper to document a detailed approach to solving the technical challenges you will inevitably face when attempting to secure any environment of this type. However, interested readers will be able to find a number of these solutions in the technical MQ focussed white paper referenced previously[1].

Six key steps to securing your middleware are presented here and they outline an approach that can be used to deliver positive change within your MOM environments.

The most important thing you must do throughout this process is to use people who understand the technology and the risks that it exposes you to. Given that middleware extends across platforms, teams and business units you are likely to need buy-in and support from the top to achieve the changes you need to make.

You are also likely to need some dedication and perseverance to see this process through. However, at the end you will be thankful that you have removed a huge blind spot from your organisation's security model and helped to ensure your business doesn't get hit by a security incident in the systems and technologies that are of critical importance to it.

The Keys to Securing Your Middleware

1. Understand the volume and criticality of the information that flows through your middleware.
2. Ask challenging questions about middleware security within your organisation.
3. Identify the threats to your business in this area and quantify the risk associated with your environment.
4. Propose solutions for those threats that will actually result in an effective reduction of risk.
5. Plan and implement the required controls across the environment.
6. Monitor and keep up to date with changing threats and alter your controls accordingly.

Conclusion

Message Oriented Middleware is a fundamental component of critical business processes for a large number of organisations. However, the risks exposed by the reliance of your business on this technology are not being correctly mitigated and this is leaving organisations with a significant exposure. It is therefore important that the security of this technology is planned and implemented effectively and that it is part of a wider risk management framework. Failure to do this could leave an organisation with unmitigated risks that could result in significant financial losses if a security incident were to occur.

References and Credits

1. MWR InfoSecurity's technical research into Websphere MQ (including a detailed white paper) can be found here: -

   http://labs.mwrinfosecurity.com/projectdetail.php?project=5

2. Information about the PCI DSS can be found here: -

   https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

3. Information about IMPACT can be found here: -

   http://www.ibm.com/impact/emedia

MWR InfoSecurity would like to thank T.Rob Wyatt for his continued help and support with their WebSphere MQ research**.**

About the Author

Martyn Ruks is the Technical Director at MWR InfoSecurity Ltd, a company which specialises in working with organisations to increase their competitive advantage through effective management of information security risk.

He has 10 years experience of performing “hands-on” security testing and assurance activities and uses as inspiration and guidance for research activities. It was whilst conducting a security testing project for a client that he first encountered IBM’s WebSphere MQ and was also where he discovered the first of several vulnerabilities affecting the software.

Martyn has conducted extensive research into IBM WebSphere MQ and has spoken at the World’s leading security conferences about the product. He is one of the foremost experts in the subject and has intimate knowledge of security weaknesses and mitigation strategies for these technologies.

As a result of his research in Middleware he has pioneered the development of security testing and auditing techniques which enable MWR InfoSecurity to offer World leading services in this space. These are continually enhanced and updated by the results of research and development activities.

The tools and methodologies that were developed have also been adopted by a range of organisations to support their internal testing and audit processes. However, increasingly it is observed that business pressures are being used as a reason to limit the security controls that are implemented, at the cost of increased risk to the business in question.

About MWR InfoSecurity

MWR InfoSecurity supply services which support our clients in identifying, managing and mitigating their Information Security risks. As a result of this approach our consultants are regularly invited to attend global technical forums to present the findings from their research.

Modern organisations are increasingly seeing Information Security as an enabler to business advantage rather than another unavoidable cost. They are responding to a demand from their customers to demonstrate that their information is secure.

MWR InfoSecurity's clients draw on our services not only because of our demonstrable expertise, but also because of the willingness and motivation of our consultants, account managers, and service managers to align themselves with an organisation's objectives. In this way we are best placed to help you manage your risk to achieve greater control and return for your business.

MWR InfoSecurity are committed to delivering information security consultancy services that utilise the latest results from research activities which is guided by new and emerging threats.

MWR Labs is the research and intelligence arm of MWR InfoSecurity which performs all technical investigations in these areas including Middleware. MWR Labs is committed to undertaking research that will assist organisations in the prevention of business threatening security breaches by exposing vulnerabilities and the methods by which they might be exploited by attackers. To achieve this it utilises the talents of some of the World's leading Information Security Researchers who employed within the technical consultancy team at MWR InfoSecurity.

This approach and close working relationship between the research capability and consultants engaged on client projects allows the effective sharing of threat and intelligence information about emerging threats on client engagements. This provides clients with up to date and accurate information about this fast moving aspect of technology and enables them to more effectively deploy resources to mitigate the risks that they face.

For the latest research and findings from MWR Labs please look at:

http://labs.mwrinfosecurity.com/notices.php

Follow MWR Labs on Twitter:

http://twitter.com/mwrlabs

MWR InfoSecurity

MWR InfoSecurity

St. Clement House
1-3 Alencon Link
Basingstoke
RG21 7SB
UK

Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083

MWR InfoSecurity
(South Africa)

PO Box 3137
Rivonia
2128
South Africa

www.mwrinfosecurity.com

If you would like to have a conversation about the topics raised in this document, please contact:

Jonathan Care
Head of Practice; Fraud, Risk and Compliance
jonathan.care@mwrinfosecurity.com

Martyn Ruks
Head of Practice; Technical Consultancy
martyn.ruks@mwrinfosecurity.com

Harry Grobbelaar
Head of Practice; Technical Consultancy,
South Africa
harry.grobbelaar@mwrinfosecurity.com

MWR INFOSECURITY