nccgroup
freedom from doubt

RESEARCH INSIGHTS

Defensive Trends

Author: James Eaton-Lee

CONTENTS

AUTHOR

James Eaton-Lee

James is a Managing Consultant within the Security Consulting team at NCC Group, where he delivers technical security, penetration testing and guidance to customers to enable them to make informed decisions about cyber defence. Prior to his role at NCC Group James was an IT Consultant, working principally with financial sector clients. James has delivered talks and training for a variety of clients on network infrastructure and security, and has co-authored two books on firewalling technology.

INTRODUCTION

Defensive measures in information security have always demanded that information security practitioners attempt to make decisive assessments as to where to deploy resources based on limited information. People, training, tools and systems may all compete for budget, and as the threat landscape changes, information security practitioners are increasingly faced with a larger potential number of places where effort may be brought to bear.

Some tools apply in a more general problem domain, helping us to refine our solutions to existing threats. By analysing data or aiding humans in working with it, we can more effectively and efficiently gain clarity regarding active threats. Other tools aid us by providing solutions to new risks in fresh parts of this landscape – or areas newly-exposed through the adoption of new technology and systems.

DEFENSIVE TRENDS

CLOUD COMPUTING

Some of the most recent trends in information security defence involve new technologies. The rise of cloud computing has brought with it new opportunities in addition to the potential for new risks outside traditional internal IT environments.

Harnessing tools such as virtualisation and leaps in broadband connectivity, it is possible for third party Cloud Service Provider's (CSP) to provide Internet-hosted services such as email, line of business applications and even entire virtual desktops. These services can be consumed by customers as if they were hosted onsite, but by utilising multiple data centres, large providers can offer platforms which decentralise infrastructure, potentially making it scalable and resilient.

By providing an always-on service, removing a requirement to own and operate or lease expensive server rooms or data centre space, and freeing up staff to focus on key business objectives, cloud computing can be an attractive value proposition.

But what threats does this outsourcing of systems and data introduce? Cloud computing is a broad term, and can refer to a vast range of third party systems. Software as a Service (SaaS) offerings may simply be shared applications – such as web applications accessed from a browser.

Platform as a Service (PaaS) offerings offer a 'managed' platform which customers may use to deploy their own applications but without the requirement to manage the underlying hosting environment, which is provided by the CSP.

At its simplest, Infrastructure as a Service (IaaS) cloud computing simply offers customers a hosted data centre environment into which they deploy their own operating systems and application stacks. The customer may benefit from the ability to scale their resource use and cloud pool, but assumes responsibility for software maintenance, hardening, etc.

Every model of cloud computing places in the hands of the vendor ultimate control of and at least some responsibility for, the underlying platform. Save for 'Private Cloud' offerings, this platform is likely to be shared with other customers – at the network level, at the server level, or indeed at the application level. A SaaS application may rely on application controls to provide separation between customers' data, whilst a PaaS offering may rely on the controls provided by other software tools such as separation enforced by virtualisation hypervisors or virtual networking.

As cloud computing increases in maturity, traditional 'core' services which were once staples of customers back office networks become increasingly tempting targets for migration into the cloud. Email and groupware tools are now routinely available as cloud-based solutions, as are Customer Relationship Management (CRM) and sales systems.

As many of these back office packages require integration with legacy or other internal systems, internal networks may also be exposed to the CSP, providing not just access to data but also a potential point of ingress to internal environments to attackers within – or with access to – the CSP.

What solutions are there to these problems?

Clearly, the segregation offered by cloud providers is likely to be a key security control, ensuring data remains separate from other commercial customers – potentially attackers or competitors.

At an application level, a focus on existing application security techniques, such as incorporation of a Secure Development Lifecycle (SDL) into application development will still provide assurance that applications' key security controls behave as intended – and that existing known vulnerability types are likely to be defended against. Penetration testing and code review of mature applications both offer empirical tests of this security, whether or not security was a key factor in development.

Most CSPs are willing to support or facilitate penetration tests; many will have undertaken these before, and may provide summaries of this testing to customers who do not wish to commission their own testing.

Customers of cloud computing services place great faith in the CSP themselves, relying on them to take care of many traditional security concerns such as system hardening, patching, and firewalling.

The Cloud Security Alliance (CSA) provides the Cloud Controls Matrix (CCM), which can be used by cloud computing customers to assess a potential (or existing) vendor and focus on security controls which may represent risk. The CSA's registry, Security, Trust & Assurance Registry (STAR), provides a publicly-available list of existing CSPs documenting security controls which they provide.

Data gathering and evaluation using a tool such as this is for many organisations a key component of procurement of services - or ongoing assessment of the security - provided by third parties. The introduction of the CCM illustrates the growing applicability of this approach to cloud offerings.

As cloud services are consumed directly via the Internet, so too are they generally managed via the Internet. Recent compromises both of individual data and organisational data have shown that procedural security and security of CSP management consoles and tools is often overlooked. Ensuring that the management channel of systems (whether cloud-based or internal) is assessed as part of any effort to secure them is of critical importance.

Increasingly, customers of cloud computing are also looking to encryption to ensure that data in the cloud is protected not only against hostile external attack, but unauthorised access from or via the CSP. While traditional database encryption may be largely ineffective against this type of threat due to the need to store key material with the data, several vendors offer solutions designed to help retain customer control of cloud-stored data, and as cloud computing matures there are likely to be more product offerings aimed at providing solutions to this problem.

DEFENSIVE TRENDS cont.

MOBILE DEVICES

Mobile computing has been increasingly mainstream for some time and many organisations are going beyond simple provision of handsets to staff, also permitting employees to utilise their own devices – handsets, tablets, and even laptops – as part of Bring Your own Device (BYoD) schemes, permitting ubiquitous access to corporate data and systems.

Some organisations provide applications to customers which are distributed freely and via vendor-specific application stores; these public services bring with them their own set of security concerns.

MOBILE DEVICE MANAGEMENT

Traditional rollouts of handsets to staff raised concerns regarding data loss, remote device configuration, hardening, remote wipe capability and encryption. BYoD rollouts compound these problems, as the handset environment is increasingly controlled by staff rather than IT and is no longer implicitly trusted or centrally controlled.

Addressing some of these concerns, Mobile Device Management (MDM) has been a key growth area in corporate IT infrastructure for some time. Early MDM software often provided simple Over The Air (OTA) configuration , device provisioning, and enterprise application delivery for corporate devices.

Today however, the state of the art in MDM often incorporates Sandboxing or Mobile Virtualisation. This technique aims to segregate personal and corporate data in BYoD environments – helping to provide assurance that corporate data is robustly stored and is less at risk from employees' personal use and cannot be accessed by other apps such as games or malware.

Increasingly, even vendors that traditionally focused on enterprise management of homogenous estates of handsets with a single Original Equipment Manufacturer (OEM) is moving towards a model of MDM which incorporates sandboxing and virtualisation across multiple vendors – allowing from multiple vendors devices to be used by staff to access corporate data with control retained by IT staff over where data is stored or transmitted and how it is protected.

MOBILE APPS

It is increasingly common for organisations across a range of sectors to make mobile applications available to their customers, in addition to mobile-friendly versions of existing websites. In these cases, organisations will have little to no control over the customer's hardware and may rely entirely on their application or the services supporting it to meet security goals.

Organisations that wish to increase or enhance their situational awareness of risk and ongoing threats would be well-advised to evaluate some of these products...

Increasing attention is therefore being paid to the security posture of these apps. There has recently been a heightened focus on ensuring that they are developed securely. In addition, increasingly sophisticated techniques are routinely being utilised to help detect jailbreaking of handsets by users (declining to allow applications to run if this has occurred) and reverse engineering (which may signify attempts to breach application security). Many of these techniques help to increase the difficulty for attackers and raise the bar in attempts to gain unauthorised access to data or systems.

In some cases, use is being made of Digital Rights Management (DRM) to protect video and audio content, in addition to strong encryption (both on the device and from client to server) to protect other forms of data at rest on the device, and in transit. While these can be useful techniques, 'home-grown' techniques are often not robust and any use of cryptography should be carefully scrutinised and where possible well-proven algorithms, libraries and toolsets should be utilised.

SIM/SEM/SIEM

Looking beyond problem spaces created by new or updated technology, it has always been a challenge to understand threats, manage logs and data, and ensure staff have situational awareness of risks and threats facing data and systems.

Security Information Management (SIM) and Security Event Management (SEM) systems such as Arcsight and NetIQ have for some time endeavoured to help organisations to solve this problem by collating and analysing data from multiple devices and sources (such as firewalls, servers, and Intrusion Detection Systems) to permit interpretation and follow-up by skilled human analysts.

SIM/SEM systems can supplement (although not necessarily replace) other administrative tools which aggregate data to aide more general IT Operations. They can be valuable in providing a better awareness of threats and attacks in real time, representing a powerful aide to security operations staff.

However, they can be challenging to work with, and it can prove difficult to extract data and integrate with other systems. Traditional commercial SIM/SEM systems are costly to implement, and require customisation, maintenance, and staff training to become – and remain – useful. They are not 'turn-key' solutions which require little to no adaptation to specific environments.

For many businesses that do not operate a full-time Security Operations Centre, large commercial SIM/SEM implementations may be out of reach. Some capable commercial offerings are aimed at smaller businesses, but may not offer some of the analytic capability or flexibility of their enterprise counterparts.

Open Source Software (OSS) alternatives to commercial SIM/SEM offerings are growing in maturity and popularity, and are increasingly backed up by commercial support and professional services offerings.

There are a wide range of mature and maintained tools aiming at information aggregation, search, and analysis.

Organisations that wish to increase or enhance their situational awareness of risk and ongoing threats would be well advised to evaluate some of these products, which are growing in sophistication and accessibility.

CONTACT US

0161 209 5200
response@nccgroup.trust
@nccgroupplc
www.nccgroup.trust

United Kingdom

Manchester - Head office
Manchester Technology Centre
Oxford Road
Manchester
M1 7EF

Cheltenham
Eagle Tower
Montpellier Drive
Cheltenham
GL50 1TA

Milton Keynes
Suite 526-528
Elder House
Eldergate
Milton Keynes
MK9 1LR

Edinburgh
37 York Place
Edinburgh
EH1 3HP

Leatherhead
Kings Court
Kingston Road
Leatherhead
KT22 7SL

Glasgow
The Beacon
176 St Vincent Street
Glasgow
G2 5SG

London
Floor 4
Tavistock House North
London
WC1H 9HR

Europe

Switzerland
Ibelweg 18A
CH-6300 Zug
Switzerland

The Netherlands
Veemkade 396
1019 HE Amsterdam
The Netherlands

Germany
Heimeranstrasse 37
D-80339 Munchen
Germany

Denmark
Tranevej 16-18
DK-2400 Kobehavn NV
Copenhagen
Denmark

North America

San Francisco
Suite 1020
123 Mission Street
San Francisco
CA 94105

Texas
4029 South Capital of Texas Hwy
Suite 100
Austin, TX 78704

New York
39 W. 14th St.
Suite 202
New York
NY 10011

Chicago
53 W.Jackson
Suite 464
Chicago, IL 60604
USA

Seattle
720 3rd Avenue
Suite 2101
Seattle

Sunnyvale
111 West Evelyn Avenue
Suite 101/103
Sunnyvale, CA 94086

Asia Pacific

Australia
2.08/56 Bowman street
Pyrmont NSW 2009
Australia

www.nccgroup.trust
@nccgroupplc