ATTACKS FROM THE INSIDE…

Righard J. Zwienenberg
Norman

Email righard.zwienenberg@Norman.com

Eddy Willems
G Data Security Labs

Email Eddy.Willems@gdata.de

ABSTRACT

Companies are (over) protecting their gateways against incoming connections. What they often forget, though, is to protect the inside of the network against all kinds of possible attacks, when there are so many external entities which have access to the internal network (contractors, telecommuters, VPN connections, etc.).

Also, lots of companies have their 'head in the clouds' – moving their services and/or servers to the cloud without realizing they have been using the cloud for a decade already and they have never given any thought to security when using services from the cloud. Even now, with financial incentives, they do not consider or look at the security implications at all.

In this presentation, we will outline and provide examples of lots of possible scenarios of internal attacks. These attacks will cost the corporate or governmental entity money, credibility, accessibility, survival or all of the above.

The possible scenarios will cover

- The human factor
- The corporate intranet
- The private and the public networks connecting to the corporate network
- The top nine problems of the 'in-the-cloud' services used by the corporate network.

INTRODUCTION

Companies often forget to protect the inside of their networks against all kinds of possible attacks, when there are so many external entities which have access to the internal network (contractors, telecommuters, VPN connections, etc.). And even with the utopia of having protection in place, it is possible to fall victim to attacks from the inside. This may be a result of receiving a 'legitimate' email with clickable content or an apparently legitimate request, for example, for information to be filled in and returned to the ISP.

SOCIAL ENGINEERING AND PRIVACY

Social engineering attacks on enterprise security systems use a combination of interpersonal skills, research and technical know-how to exploit human nature to breach corporate and personal privacy. As social engineering involves getting information from the inside it can be seen as an example of an attack from the inside.

Social engineering involves the manipulation of people rather than technology to successfully breach an enterprise's security. Despite our advances in technology, social engineering remains the single greatest security risk, and many of the most damaging security breaches are the result of social engineering, not electronic 'hacking' or 'cracking'. Many hacking attacks are based on social engineering.

Social engineering depends on an understanding of human behaviour, and on the ability to persuade others to release information or perform actions on the attacker's behalf. Persuasion itself is an art and a science; studies show that humans have certain behavioural tendencies that are exploitable via careful manipulation. Some individuals possess a natural ability to manipulate, while others develop the skill through practice using positive (and negative) reinforcement. Social engineering attackers play on these tendencies and motivators to elicit certain responses in the target. A study published in *Scientific American* (February 2001) cites five basic tendencies of human behaviour that help generate a positive response:

- reciprocation: you give a freebie and want to do something with it
- consistency: certain behaviour patterns are consistent
- social validation: everybody behaves in the same way
- liking: people tend to say 'yes' to those they like
- scarcity: someone in low supply will become precious.

Anything that stores or accesses information is vulnerable to a social engineering attack, and no person at any level of the enterprise is safe. While an old invoice or phone list may not seem dangerous in and of itself, an attacker can use this information to develop a relationship by showing 'inside' knowledge as a way of gaining short-term trust. Electronic systems are subject to direct attack or probing. Learning a system name or IP number may allow an attacker to present himself or herself as a network technician, and a large amount of information on your enterprise or personnel is probably available on the Internet in public or private databases. Social engineering attackers can often gain at least limited access to enterprise systems, even if it's just by looking over someone's shoulder during an on-site visit. Every little scrap of information is valuable to an attacker. It's important to remember that social engineering attacks are cyclical, with attackers slowly gaining information with each cycle until they reach their target. Information can be public or private, sensitive or non-sensitive, secure or non-secure. Unfortunately, there are large amounts of information that are public, sensitive and non-secure, such as financial data, personal data, platform details for systems and networks, and leaked secret documents. Malicious individuals have always known that the best way around any security system is to manipulate a human target into giving them what they want – what we call social engineering. It remains the single greatest security threat to enterprises. Security-aware employees, strong authentication, and effective checks and balances are the most effective methods to defend against internal and external social engineering attacks.

SOCIAL NETWORKING PROBLEMS

Everybody is attracted by social networks such as *Facebook* or *MySpace*. The intention of these sites is for users to keep in touch with existing friends, exchange information, and also search for new friends. There are also a lot of other sites, e.g. *LinkedIn*, used for maintaining business contacts or searching for old school friends. Social networks are great places to meet and network with people who share similar business interests but they are also very dangerous to users and their companies. Many businesses view social networking sites as a kind of online cocktail party: a friendly, comfortable place where one can establish contacts, find buyers or sellers, and raise a personal or corporate profile. But the cocktail party metaphor isn't entirely accurate. In fact, users would be better served if they thought of social network services as a loud glass house; a place with endless visibility and each occupant talking through a highly amplified horn. Since most people access social network sites from the comfort and privacy of their home or office, they can be lulled into a false sense of anonymity. Additionally, the lack of physical contact on social network sites can lower users' natural defences, leading individuals into disclosing business or private information they would never think of revealing to a person they just met on the street or at a cocktail party.

Over-sharing company activities

When someone gets excited about something their company is working on and simply must tell everyone about it, a problem arises. By sharing too much about your employer's intellectual property, you threaten to put them out of business by tipping off a competitor who could then find a way to duplicate the effort or to spoil what they can't have by hiring a hacker to penetrate the network. Then there are hackers controlling botnets that could be programmed to scour a company's defences and, upon finding a weakness, exploit it to access data relating to intellectual property. With the data in hand, the hacker can then sell what they have to the highest bidder, which just might be your biggest competitor. Sharing this kind of information could lead to targeted attacks on specific technology-producing enterprises.

Mixing personal with professional

This problem is closely related to the first, but extends beyond the mere disclosure of company data. This is the case where someone uses a social network for both business and pleasure, most commonly on *Facebook*, where one's 'friends' include business associates, family members and friends. The problem is that the language and images one shares with friends and family may be entirely inappropriate on the professional side. A prospective employer may choose to skip to the next candidate after seeing pictures of you drunk or showing off a little too much leg at someone's birthday party. In sharing such things, you also stand a good chance of making the company you represent look bad. In some cases, it's nearly impossible to separate the business from the personal on a social networking site. Those who work for media companies, for example, are sometimes required to use all their social networking portals to proliferate content in an effort to boost page views which, in turn, attracts potential advertisers. But wherever and whenever possible, security practitioners work to keep people locked in their respective boxes.

Most connections?

For some social networkers, it's all about accumulating as many connections as possible. Folks on *LinkedIn* are notorious for doing this, especially those in some specific *LinkedIn* groups. This may seem harmless enough or, at the worst, just annoying. But when the name of the game is quantity over quality, it's easy to link with or accept a 'friend' request from a scam artist, terrorist or identity thief.

Clicking on everything

Facebook and *Twitter* in particular are notorious as places where inboxes are stuffed with everything from drink requests to requests to join a cause. For some social networkers, clicking on such requests is as natural as breathing. Unfortunately, the bad guys know this and will send links that appear to be from legitimate friends. Open the link and you're inviting a piece of malware to infect your machine.

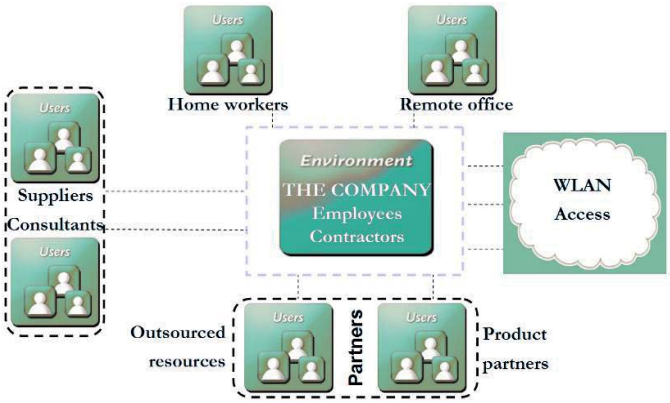
Endangering yourself and others

Reckless social networking can literally put someone's life in danger. It could be a relative or co-worker. Or it could be you. It's advisable and logical to pay extreme caution when posting birthday information, too much detail on your spouse and children, etc. Otherwise, they could become the target of an identity thief, etc.

TODAY'S NETWORKS LACK CLEAR, CRISP BOUNDARIES

Where does a network stop these days? Where does the business network stop? This is not so easy to define any more. Most of us can work easily from home through a secured VPN connection. But that's not always the case. Some companies are opening up parts of the network to the outside world. Users are logging into their companies' mail systems in open public places to check their email. It's obvious, of course, that password stealers and other spyware could easily be used to reveal the real login and password details, giving any hacker access to inside information from the company. Other problems come increasingly from mobile devices, on which email checking is routine these days but which can even be used to log into a terminal server. If used on a public network it could easily be sniffed to reveal the login details to the hacker who's drinking a cappuccino in the same coffee shop where you are checking your mail. Most of us have good protection in place at home but a lot of people don't think about these possible problems in public places. As today's networks lack clear, crisp boundaries it becomes more and more difficult to define the real inside and outside of the corporate network. It even becomes more and more difficult for normal users to protect themselves and to detect the real risks behind every part of the network. This issue is likely to increase and will become more and more problematic in the coming years.

If we take a look at what today is a common network for corporate use, we can see several problems at hand:



The network segments, both internal and external, are so interconnected that any kind of infection will spread throughout the network; any kind of trojan enumerating the network for open shares will find them, etc. Over the years, most malware attacking corporate intranets has spread over three well known protocols: CIFS, SMB and RPC.

Now, you may have all possible security measures in place such as user training, patch management, hardware remediation and anti-malware management, but with new types of hardware and unknown risks, new infections may infest your intranet using the aforementioned protocols or other commonly used protocols such as HTTP, FTP, SMTP, TFTP, POP3, IRC, etc. The best way to counter this potential malicious vector is to use a network-transparent real-time malware scanner – or better, an In-Line Network Content Scanner. This device should be invisible (promiscuous mode) and with the knowledge of the different protocols be able to scan traffic using these protocols.

Placing this device at strategic locations will minimize the risk as infections can be detected earlier, can be contained to a smaller network segment, or can even protect legacy networks (networks running systems with old operating systems that may still be vulnerable to attacks as they understand (some of) the protocols and for which no anti-malware software is available any more).

THE CLOUD

Working definition of cloud computing

This is the working definition of cloud computing we are using for the purposes of this study. It is not intended as yet another definitive definition [1]:

> Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies. Cloud computing architectures have highly abstracted resources, near instant scalability and flexibility, near instantaneous provisioning, shared resources (hardware, database, memory, etc.), 'service on demand' usually with a 'pay as you go' billing system, programmatic management.

There are three categories of cloud computing:

- **Software as a Service (SaaS):** SaaS is software offered by a third-party provider, available on demand, usually via the Internet and remotely configurable. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (*Google Docs*, etc.).
- **Platform as a Service (PaaS):** PaaS allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management and deployment platforms. (*Microsoft Azure*, *Google App* engine, etc.)
- **Infrastructure as a Service (IaaS):** IaaS provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. (*Terremark Enterprise Cloud*, *Windows Live Skydrive*, *Rackspace Cloud*, etc.)

SECURITY BENEFITS OF CLOUD COMPUTING

The security benefits of cloud computing include:

- The benefits of scale and rapid smart scaling of resources
- Standardized interfaces for managed security services
- Audit and evidence gathering
- More timely, effective and efficient updates and defaults.

TOP nine 'in-the-cloud' problems

It is hardly necessary to repeat the extensive material which has been written on the economic, technical, architectural and ecological benefits of cloud computing. An examination of the security problems related to cloud computing, as has recently been reported in news from the 'real world', must be balanced by a review of its specific security benefits. Cloud computing has significant potential to improve security and resilience, however special care must be taken with regard to several upcoming threats. We will try to give you an overview of the most important 'in-the-cloud' problems [2].

#9 Identity management

You can never be sure who really is who. Attackers can misuse your identity. The cloud does not really know who you (physically) are. If attackers can gain access to your network, they can communicate with the cloud. As the cloud thinks it is still communicating with a trusted source (your network), lots of information can be intercepted or the cloud can be fed with lots of faulty data.

Another possibility is an identity management man-in-the-middle attack where the attacker is between the network (victim) and the cloud.

#8 Nefarious use of service

Providers offer their customers the illusion of unlimited computing, network and storage capacity often coupled with an easy registration process where anyone with a valid credit card

can register and immediately begin using cloud services. Some of them even offer free trials. By abusing the relative anonymity behind these registration and usage models criminals have been able to conduct their activities, sometimes without any problems. Current and future areas of concern include password and key cracking, DDoS, launching dynamic attack points, hosting malicious data, botnet command and control centres and CAPTCHA-solving farms. Good examples of this problem are the service providers who have hosted the Zeus botnet and download for *Microsoft Office*, *Adobe* PDF exploits, etc. Additionally botnets have used IaaS servers for command and control functions. Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud computing providers are actively being targeted because their easy and weak registration systems facilitate anonymity and because providers' fraud detection capabilities are limited [3].

#7 Account/service hijacking

If the cloud account or service is hijacked one way or the other, it can be misused for almost any kind of malicious intent, depending on the original service of the cloud. Whenever this happens, it can have very nasty consequences for both the user and the company that get hit. Eventually, the owner of the account will be blamed. A classic example of this is the (in)famous Twittergate.

#6 Financial DDoS

There are several different scenarios in which a cloud customer's resources may be used by other parties in a malicious way that has a financial impact:

- Identity theft: an attacker uses an account and uses the customer's resources for his own gain or in order to damage the customer economically.
- The cloud customer has not set effective limits on the use of paid resources and experiences unexpected loads on these resources through no malicious actions.
- An attacker uses a public channel to use up the customer's metered resources – for example, where the customer pays per HTTP request; a DDoS attack can have this effect.

A financial DDoS destroys economic resources; the worst case scenario would be the bankruptcy of the customer or a serious economic impact.

#5 Data loss/data leakage

Imagine a document containing classified information being stored or being scanned in the cloud. Who is behind the cloud? Everything that happens within your company can be controlled – you control what goes out, but what happens when it gets to the cloud? Is it forwarded automatically to 'someone' or 'something' else? If it is scanned in the cloud and is misidentified (false positive), will it be quarantined in the cloud?

#4 Unknown risk profile

One of the advantages of cloud computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the security concerns. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts and security design, are all important factors for estimating your company's security position. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposure. It may also impair the in-depth analysis required in highly controlled or regulated operational areas. When adopting a cloud service, the features and functionality may be well displayed, but what about details or compliance of the internal security procedures, configuration hardening and patching? How are your data and related logs stored and who has access to them? What information, if any, will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile. A clear example of this problem is the *Heartland* data breach: *Heartland*'s payment processing systems were using known-vulnerable software and actually infected, but *Heartland* was 'willing to do only the bare minimum and comply with state laws instead of taking the extra effort to notify every single customer, regardless of law, about whether their data has been stolen.' [4, 5].

#3 Hidden logs/intrusion attempts

A direct attack aimed at a company's network will be noted and is visible in the gateway log files. But what if the attack is aimed at the cloud? An attacker could forward all messages to himself; nothing of this gets noticed in the company's gateway log files.

#2 Insider abuse

The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kinds of data, IP and services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. This can be considered especially important in the case of cloud computing due to the fact that cloud architectures necessitate certain employee roles which are extremely high risk. Examples of such roles include system administrators and auditors and managed security service providers dealing with intrusion detection reports and incident responses. As cloud use increases, employees of cloud providers increasingly become targets for the cybercrime community. For in-the-cloud companies insider abuse carries more risks than for normal businesses as the impact itself could be much wider and targeting several companies instead of one in particular. The vulnerabilities here are clear and range from unclear roles, system or OS vulnerabilities, inadequate physical security procedures to application problems or even poor patch management. To complicate matters, there is often little or no visibility regarding the hiring standards and practices for cloud employees. It is clear that the level of access granted could enable a criminal to harvest confidential data or gain complete control over the cloud services with little or no risk of detection. It is also clear that several problems like these are mostly not

conveyed to the public as this could have too large a financial impact on the 'in-the-cloud' service provider [6].

#1 Centralized AAA Abuse/Trust (Authentication, Authorization and Accounting)

Authentication, authorization and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. If the AAA cannot be guaranteed, e.g. if an account is hijacked, this will be put on the holder's account and all 'trust' on his name.

CONCLUSION

No matter how hard you try to protect your network against attacks from the inside, there are still plenty of ways in which these attacks can occur. Unknown third parties or services with unknown risk profiles, rogue employees and social engineering are all things which can and actually are taking place in attacks on your network – attacks starting from the inside…

REFERENCES

[1] 'Cloud computing, benefits, risks and recommendations' ENISA Whitepaper November 2009 p.14.

[2] http//www.cloudsecurityalliance.org/.

[3] http://www.malwaredomainlist.com/, http://blogs.zdnet.com/security/?p=5110.

[4] http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349670,00.html, http://chenxiwang.wordpress.com/2009/11/24/follow-up-cloudsecurity/, http://www.forrester.com/cloudsecuritywebinar, http://www.cerias.purdue.edu/site/blog/post/symposium_summary_security_in_the_cloud_panel/.

[5] http://www.pcworld.com/article/158038/heartland_has_no_heart_for_violated_customers.html.

[6] http://www.programmableweb.com and http://securitylabs.websense.com/content/Blogs/3402.aspx.