WEB RISK EXPOSURE – DON'T FORGET YOUR INTRANET

DANNY ALLAN, STRATEGIC RESEARCH ANALYST

A whitepaper from Watchfire

TABLE OF CONTENTS

INTRODUCTION

Intranets are an efficient, effective way to communicate, store knowledge and generally boost employee productivity. According to IDC, more than 89 percent of large companies have an intranet.[1] But there's a growing downside. This sprawling, highly distributed system is loaded with confidential, sensitive and even inappropriate content – financial data, employee health records, customer account or credit card numbers. This is content that may be accessible to everyone in your company – including disgruntled employees and temporary contractors. IDC claims that more than 50 percent of large enterprises have needed to terminate employees or contractors for internal security violations on their intranets. Additionally, many non-employees (contractors, partners, etc.) have access to the corporate intranet. These interactions must be documented to ensure protection and compliance.[2]

It is therefore critical to monitor and manage content on your intranet – automatically and reliably – and to understand your intranet environment – what you have, and where it's located. It is also imperative to reduce the risks associated with easy access to this sensitive content. This paper will discuss the risks associated with the intranet and will provide best practices to help defend against threats.

THE CHANGING STATE OF THE INTRANET

Intranets have long been an efficient way to disseminate information across organizations as well as an effective way to share information and promote collaboration. It is not uncommon for many people to have permissions to publish information to the intranet and often with very little QA required. This self-serve approach reduces the need for a specific team to be dedicated as the "gatekeeper" for information delivery within an organization.

The growing risk is that there may be no control over what content and applications become publicly available and the challenge is how to effectively manage this infrastructure. The challenge is further complicated with increased regulatory pressures (from legislation such as HIPAA, GLBA, Sarbanes-Oxley), growing demands for IT to improve and secure access to critical data, and the disappearing "perimeter" that once defined intranets.

THREAT MODELING FOR THE INTRANET

Threat modeling for the intranet can help you identify and rate any threats that may apply to your intranet. In web application security, threat modeling is the systematic identification and rating of threats most likely to impact your system. This task is completed for the purpose of understanding the risk associated with the application, and implementing needed countermeasures. The same principle of threat modeling can be applied to the intranet as a whole. There are very real threats that are introduced by the intranet. Understanding and identifying these threats, and knowing and implementing the proper countermeasures, are all essential tasks associated with managing the intranet.

Threat modeling for the intranet involves *six steps*:

- Identify assets

[1] "What's Happening Inside – 10 Major Intranet Trends and What We Can Learn from Them," *CIO*. http://www.cio.com/intranet/edit/intranet_trends.html

[2] "Security and Regulatory Compliance – Don't Forget Your Intranet," by Charles Kolodgy, IDC Viewpoint, May 2005. http://www.idc.com/getdoc.jsp?containerId=VWP000250

- Create an intranet overview
- Decompose the intranet
- Identify threats
- Document the threats
- Rate the threats

Step 1: Identify Assets
The first step is to identify the assets that compose your intranet. These may include:

- **Physical Assets:** anything that is a physical/tangible object on the intranet (i.e. web infrastructure (network, web servers), application, FTP servers)
- **Applications and content**: effective analysis of the content can only be completed when a comprehensive inventory of the content and applications composing the intranet have been identified.
- **Confidential data:** this includes everything from customer information (e.g., credit cards, SSNs), account numbers, employee data (e.g., employee files, medical records, payroll data) to intellectual property owned by the company.
- **System Resources & Availability**: less tangible assets that are a crucial part of the intranet are system resources and availability. No longer is it simply sufficient to ensure the physical assets are running, but intranet continuity ensures that critical applications are available when and where needed.

Step 2: Create an intranet overview
It is important to identify the purpose of your intranet. As a part of this exercise, list what these purposes are and create an intranet diagram. Simply identifying the purposes of your intranet may reveal applications and content that are costing time, resources and money, but are not fundamentally needed. Intranets that exceed the goals and purposes of the organization could constitute unnecessary risk.

A second task to be completed is to loosely map the goals and purposes of the intranet to the applications and technologies identified as part of Step One. Early definition of this mapping will better enable the organization to successfully complete the next step. As an example, consider the Human Resources application which must be secured so that individuals only have access to their own personal data. The goal of the application is to provide secure, self-service to the employee without compromising any other employee's data. Without mapping this application to the authorization technologies that restrict access, it is impossible to begin the decomposition of the intranet and establishing trust boundaries.

Step 3: Decompose the intranet
The decomposition process is where you determine where the "trust" boundaries on your intranet begin and end. A trust boundary is simply a location where the level of trust changes. Identify the systems, subsystems and identities that your intranet trusts. This process is important to ensure that only authorized individuals are allowed within the trust boundary. Consider these questions:

- ***Who has access*? –** is all the information on the intranet available to everyone, or are there some areas that are restricted to individuals?
- ***Where does the information go*? –** does the information stay within the Customer Relationship Management (CRM) system, or do individuals have the ability to download the information from the intranet to a local computer that travels home with them?
- ***Are there external integrations*? –** do you have information stored on your intranet that is integrated with a third-party system (e.g., analytics)?

- ***Is there any privileged data on the intranet*? –** where is and what is the privileged data that I have on my intranet, and what are the access and entry points that I have in place to determine my data flow for identifying these assets? Consider a web-enabled CRM automation software package that collects sales information for the entire organization. Individual account managers would absolutely require access to their sales and account information, while exposing the entire organization pipeline and sales information to an account manager who was soon to leave the company. This could constitute a serious risk.

Step 4: Identify Threats
It is important to identify the threats that might compromise the system and assets before you mitigate the risks against them. To do this, you will need a cross-organizational team to categorize and brainstorm the threats – people from across the organization (marketing, IT, etc) that will know the underlying system, infrastructure and content and can best determine what the threats are. It is important to identify the threats by type:

- **Network** (switches, router, firewall): Certain threats may apply specifically to the underlying network of the intranet. These would include threats such as malicious triggers and payloads that compromise the software on these network assets, or packet spoofing.
- **Host** (patches, shares, user access): The host is the actual physical asset on which intranet applications and content are hosted. Certain threats might be targeted toward the host. These would include issues such as Buffer Overflows and illegal paths.
- **Application** (SQL injection, XSS): The application sits at the very top of the intranet infrastructure. Since this is the "front" to the employee, there are many and varied threats that directly impact the application. The Web Application Security Consortium (WASC) publishes a specific Threat Classification list that categorizes these threats including Client-side Attacks and Command Execution.[3]

Step 5: Document the Threats
Determining the threats and documenting the system will return a list that is infinitely long. The following grid is an example of how you can document these threats.

Threat Description	**Access to sensitive client data**
Threat target	Credit card information in client database
Attack techniques	Simple search using intranet search engine for client names
Countermeasures	• Identify information and enforce authentification/authorization • Scan intranet with search engine using least privilege • Use regex on reverse IDS to scan for credit card values – IDS is an intrusion detection system that looks at data crossing the network
Regulatory impact	GLBA

[3] http://www.webappsec.org/

Step 6: Rate the Threats
There are two well-defined methods for rating threats: the **Risk** method and the **DREAD** method.

Many Risk formulas have evolved over time. Choosing the correct formula is dependent upon the organization.

Risk = Probability*Damage Potential

This method enables you to mitigate your highest threats first where:

- Probability: 1 = unlikely, 10 = near certainty
- Damage: 1 = minimal, 10 = catastrophic

The **DREAD** method is a more involved classification of risk and stands for:

- **D**amage potential – the damage potential of the attack
- **R**eproducibility – how easy it is to reproduce the attack
- **E**xploitability – how easy it is to exploit the attack
- **A**ffected users – very important when you're talking about the risks to your client base or to employees
- **D**iscoverability – how easy it is to discover the attack

Each one of these categories is given a rating of 1-3 (with an overall total of 15) – and those issues with a rating near 15 are mitigated before those at the lower end of the scale.

COUNTERMEASURES

Most companies will more than likely look to mitigate risk on their public-facing Internet before addressing intranet threats. Internet applications and content may be exposed to a far greater audience than the intranet, but it is important to note that recent research reports that more than 30 percent of all organizations report at least one security incident beginning within the organization, while 24 percent reported a security incident, but could not determine the origin.[4] Companies should select the top risks to the intranet and begin to manage these risks using identified countermeasures. They can buy some assurance by implementing systems which will protect them, but if they have threats that have already become vulnerabilities, they will have to consider software that monitors web application vulnerabilities to help fix and prioritize the issues most critical to the organization.

Keep in mind that while it is never wrong to use technology in this process, relying *exclusively* on the technology is not enough to manage this risk. It is critical to rate these threats and then determine the highest potential risks accurately. Appoint the necessary people in your organization to determine the most likely threats and those that will likely incur the highest damage, and delegate the implementation of countermeasures appropriately.

PERIMETER PRINCIPLES

1. **Perimeter defenses for the intranet do not work if the perimeter is too large.** Defenses for large organizations with a huge perimeter of millions of pages and thousands of applications simply do not

[4] 2005 CSI/FBI Computer Crime and Security Survey (p. 13).
http://www.cybercrime.gov/FBI2005.pdf

work. With so many people (employees, outside contractors, etc.), the perimeter defense is really not a defense. Remember that more than 50 percent of large organizations have needed to terminate employees because of security violations on their intranets where at least one person was willing to compromise internal security, and as these organizations continue to expand, intranet security becomes extremely difficult to manage.[5]

2. **Small "enclaves" are much better.** Small enclaves for intranets are much better to manage. The smaller the area where the information is kept, the easier it is to defend. It is much easier to defend against a small network segment than a large, distributed intranet.
3. **Implement in the same way as the Internet.** Keep in mind the same implementation best practices for your intranet as you would the Internet (i.e., the routing restrictions, firewalls, encryption, etc.).
4. **Consider the perimeter "gone."** The concept of a perimeter has been introduced by many organizations through the usage of firewalls and network topology. Over the past five years, however, the massive shift toward pervasive connectivity has eliminated this perimeter. The idea that only internal and known computers can access certain systems is no longer valid. Today, employees are able to connect remotely through virtual private networks, secured connections, wireless devices and personal electronic devices. The employee might be at their desk, at home or in a public airport. This does not include those contractors, temporary employees or third-party business partners which require some form of access into internal systems. The perimeter truly does no longer exist.

PROCESS PRINCIPLES

Be sure to implement applications for the intranet using Enterprise Risk Management programs. Use a very systematic approach which considers threat modeling for the intranet – **Discovery, Asset Analysis, Usage Analysis** and **Secure**:

- **Discovery** – discover all the assets within your organization, and do not be afraid to use technology.
- **Asset Analysis** – analyze all assets, and do not be afraid to use technology.
- **Usage Analysis** – consider a monitoring process that analyzes the traffic that crosses the network, where people are going and how they are going there, and content consolidation.
- **Secure** – organizations need to ensure that they have authorization in place so people only have access to what they should have access to as well as authentification processes for accessing content.

CONTENT PRINCIPLES

1. **Less is more.** As intranets continue to grow and expand exponentially, everyone becomes a contributor. It is critical that organizations control the growth of their intranets.
2. **Consolidate wherever possible.** Consolidate your intranet and keep it as controlled as possible. Intranets today can be tens of thousands of pages and are usually 10 times the size of an organization's Internet. The reason for this is because so many employees have access to publishing information, and they think it's useful to post it all on the intranet. The truth is that the more content that is up on the intranet, the harder it is to find information and the more difficult it is to defend against threats.
3. **Document information shelf life.** Make sure to remove outdated material from your intranet. This out-of-date material could be taking up system resources and poses a risk to the organization. It is

[5] "Security and Regulatory Compliance – Don't Forget Your Intranet," by Charles Kolodgy, IDC Viewpoint, May 2005. http://www.idc.com/getdoc.jsp?containerId=VWP000250

also a good idea to introduce shelf-life dates on content. For example, every document posted on the intranet should have a "use before" date at which time the document is removed.

SUMMARY

Intranets are an efficient and effective way to communicate and boost employee productivity, but they can also present one of the greatest risks to your organization. Consider the perimeter as "gone" with the intranet and that everyone has access as a baseline to manage the web risk exposure for your intranet. Also apply a simple threat modeling approach to the intranet:

- Discover
- Analyze
- Secure

And remember that less is more for the intranet. Don't be afraid to use technology when monitoring and managing your intranet risk, but do not only rely on technology. Organizations need to understand that a combination of the appropriate processes and technology will help best mitigate their intranet risk.

ABOUT WATCHFIRE

Watchfire provides Online Risk Management software and services to help ensure the security and compliance of websites. More than 500 enterprises and government agencies, including AXA Financial, SunTrust, HSBC, Vodafone, Veterans Affairs and Dell rely on Watchfire to audit and report on issues impacting their online business. Watchfire has been the recipient of several industry honors including the HP/IAPP Privacy Innovation Award, *InfoSecurity Product Guide*'s Hot Security Company 2006, *Computerworld*'s Innovative Technology Award, "Recommended" rating by *Computer Reseller News*, finalist in *SC Magazine* Awards 2006. Watchfire was named by IDC as the worldwide market share leader in web application vulnerability assessment software. Watchfire's partners include IBM Global Services, PricewaterhouseCoopers, Sapient, TRUSTe, Microsoft, Interwoven, EMC Documentum and Mercury. Watchfire is headquartered in Waltham, MA. For more information, please visit www.watchfire.com.

