REVISITING CONNECTIVITY THREATS IN SECURING KNOWLEDGE MANAGEMENT SYSTEMS

Brett J. L. Landry
College of Business, University of Dallas
1845 East Northgate Drive, Irving, TX 75062
blandry@udallas.edu 972-636-8633

M. Scott Koger
NOAA National Climatic Data Center (NCDC)
151 Patton Avenue, Asheville, NC 28801-5001
scott.koger@noaa.gov 828-350-2024

ABSTRACT

There is a common misconception that internal IP networks (intranets) are secure; and that external networks such as the Internet and extranets are vulnerable and unsecured. The truth of the matter is that networked information assets are at risk no matter where they reside. With increases in the availability of connectivity, collaborative computing, and shared knowledge bases, the problems are compounded. Traditional reliance on appliance oriented, perimeter based security has proven to be ineffective in securing information in todayôs highly connected and increasingly porous environments. The information asset is now the perimeter. The very nature of devices being networked makes them vulnerable on an IP network to various attacks and spoofs. This paper reexamines the validity of the application of the P-I-E model to identify and examine threats to knowledge management systems from private, Internet, and enterprise sources.

INTRODUCTION

There is a common misconception that internal IP networks (intranets) are secure; and that external networks such as the Internet and extranets are vulnerable and unsecured. The very nature of the persistent ñalways onò connections of IP aware devices makes them vulnerable to an increasing array of attacks and spoofs. With the emergence of truly ubiquitous networks and increasingly capable personal electronic devices, there continues to be an arms race in protecting and securing the enterprise network. Depending on the environment, there can be more entry and egress points on the network as there are users. It is not at all uncommon to find a knowledge worker or student with three or more network aware devices in their possession, many of which are quietly riding our enterprise networks out to the Internet, and more concerning ï in many cases, things on the Internet are riding them back in.

An enterprise is not a single network. It is a federation of networks among various business partners, functional, organizational, or geographic units combining network resources, shared knowledge bases, as well as risks and vulnerabilities. The risk tolerance, level of sophistication, and depth of security expertise can vary wildly among these different networks but it is important to remember that they are each only as strong as the weakest among them. Repeatedly

over the last several years, stories have reached the press of attacks against the weakest link in the enterprise leading to major intrusions, data breaches, and loss of intellectual property. TJ Maxx, Heartland, and more recently Sony, RSA, and DigiNotar are all examples where attackers were able to leverage one or more weaknesses in a network or system to gain access to other systems and eventually reach valuable information assets. The concern is no longer over just desktops and laptops, or even unmanaged home machines, but from PDAs, smart phones, tablets, and a continuously evolving ecosystem of networked and mobile devices. The vending machine down the hall, the HVAC controller, and the smartphone in a userôs pocket all pose threats to the enterprise network environment. This paper will use the model proposed by Landry, Blanke, Koger, & Nielsen (2008) to examine the threats to Knowledge Management Systems (KMS).

The landscape has dynamically and dramatically changed over the last two decades with the adoption of the WWW, Peer-to-Peer (P2P) file sharing, ubiquitous wireless access, and most recently Voice over IP (VOIP). Wireless Ethernet (WIFI) has redefined the boundaries of the network with internal network access outside the perimeter of the organization. Personal mobile hotspots like 3 and 4G MIFI, cellular modems in laptops and other portables present a problem for detection and prevention. Cellular modems and smart phones with tethering enabled can act as network bridges between the Internet and the intranet. An additional concern is the fragmented operating system environment. Users are usually dependent on their cell service provider to make software updates available, and the lack of widely available antivirus or anti-malware protection continue to make Windows Phone 7, Android, and even iOS across multiple generations of devices susceptible even after security updates are released. These devices routinely leave the intranet and go to the Internet and to home networks (whether at home or other private locations). As a result, traditional techniques at securing KMSs are no longer effective.

Broadly speaking the term knowledge management system can be applied to anything from simple shared files on a network, to content management (CMS) and learning management (LMS) systems, to the most robust cloud based services. Ideally these environments provide a set of capabilities and tools where ad hoc groups of individuals or organizations can collaborate, archive, and control access to informational assets ï be it simple document repositories, multimedia, instructional and creative content, business or legally sensitive information that require some common set of access controls. Frequently these systems offer some form of version control and audit capabilities. Security is a huge concern within KMSs because both the tremendous value of intellectual property and the liability of personal identifiable information leakage. Additionally, KMSs are being extended by remote access and by mobile devices, where users can take the content with them. This redefines the perimeter of the KMS and the network security. Because of these reasons, KMSs must be protected in a secure fashion by identifying threats from a number of sources.

The Private -Internet - Enterprise (PIE) model was developed to address the reality that security threats come from other sources than just internet firewalls access. The model accepts that there are shared risks among constituents. These main three groups are the enterprise network, the Internet, and the private networks that are not part of the Internet or the enterprise Intranet. Using the PIE model as shown in Figure 1, threats to a KMS can be more easily identified and prioritized for mitigation. The areas of greatest concern are at the intersections of these

computing environments. The four intersections are security concerns, however only three of the four zones are within our control. There is no control or dominion over what happens between the Internet and Private Networks because it is outside of our intersection, but is still a concern to protecting KMS. Each of these seven realms will be discussed below.

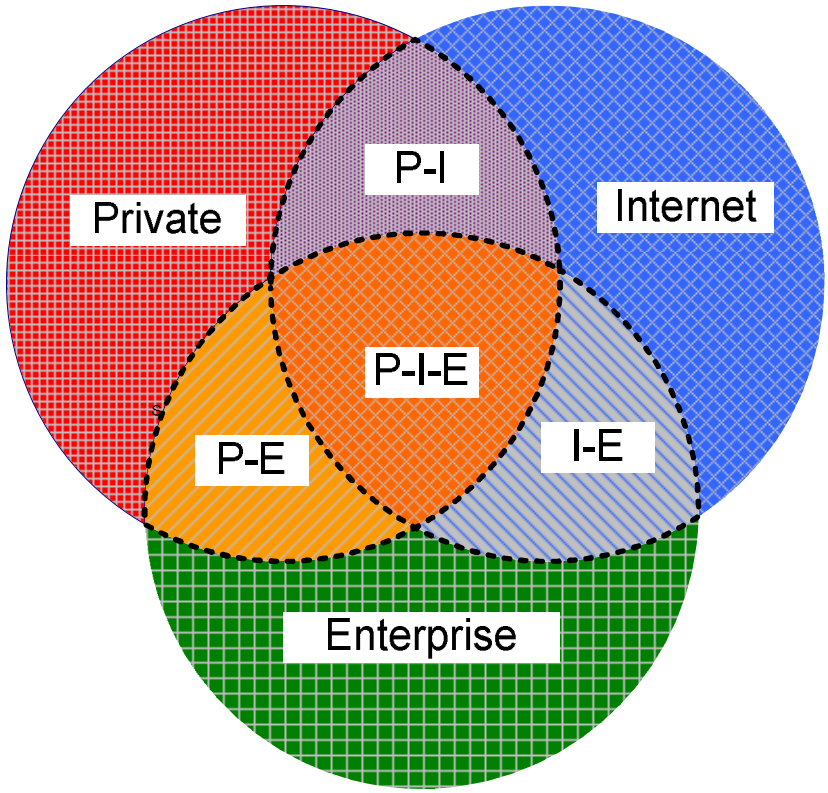

Figure 1: The PIE Model

Traditional network security addresses some of these concerns through the use of hardware and software access controls as well as security policies. While computing processes may occur in a secure environment, once inputs or outputs from those environments occur, risks to confidentiality and integrity of a KMS exist. Where once KMSs were largely confined to a single network, they are now frequently shared by multiple organizations, often across unsecured networks. To compound the issue, employees access these resources from beyond the enterprise boundaries. An examination of the intersections between the traditionally secured enterprise network and the current environment can offer insights into the threats posed against KMS assets.

Private (P)

Private networks are everything that is not part of the enterprise or on the Internet, and has at least one responsible party for their maintenance (this could be a multinational firm or a small office / home office). Private networks are only as secure as their users make them. There are usually no regulatory or compliance requirements for minimum security measures as there are with business networks, e.g. PCI compliance for businesses that accept credit card payments. These networks are usually vulnerable to most threats from the Internet and serve as vectors for viruses and worms.

The problem with private machines is that no one entity is responsible for them. These machines become fertile breeding grounds for robot networks, called botnets. Botnets are small to very large scale collections of compromised computers often used to create Distributed Denial of Service attacks (DDoS) or mass spam mailings. The system owners are typically unaware that their computers are infected and are being used for illegal purposes. While recent arrests have cracked down on master botnets, there is no way to catch all the perpetrators as this has the potential to be a moving growing target around the world. The private realm is a concern because the users with access to the KMS are outside of the organizational defenses and are not subject to the security measures contained within the enterprise.

Internet (I)

The Internet is the realm from which most malware and other cyber threats emerge. While the early years of Internet connectivity were predominately marked by virus and worm infections, the Internet today is increasingly focused on illicit profit. Criminal organizations have recognized the potential profit in blackmail, spam, and theft of financial data. The use of sophisticated collections of botnets give criminals isolation from easy tracing, yet provide an almost free platform for launching attacks. In addition, international laws have failed to keep pace with the level of threat posed by economically motivated cybercrime. Many cybercriminal organizations operate out of countries that either have weak laws, weak enforcement, or both. Criminal organizations are distributing free software that looks legitimate but secretly installs Trojan horse programs such as key loggers, bot clients, or other spyware. The unfortunate victimsô compromised machines are then used to send spam email or worse, collect password and financial information used to steal identities or empty bank accounts.

Enterprise (E)

Traditional network security addresses some of these concerns through the use of hardware and software access controls as well as security policies. Unfortunately these traditional methods have proven to be insufficient at protecting the organizationôs KMS in the new environment. Risks have increased due to the proliferation of portable devices and increasingly powerful personal computing products. The enterprise realm is the only area of the new computing environment where a significant degree of control is available. With corporate resources dedicated to securing the enterprise network and strong corporate policies enforcing security some measure of control can be obtained. Traditionally focused on external threats, the enterprise must now shift focus to more complex threats both internal and external sources.

Private – Enterprise (P-E)

When private users connect to the enterprise network there is an intersection of these two realms as indicated in Figure 1. These users may be partners, suppliers, or other known users connecting from home machines on private or open public networks (coffee shops, etc) using open Internet connections, dialup, or VPN connections to connect to the KMS. While we know who the user base should be, we have limited or no control over the security configuration of the devices they use to connect or the networks they connect from. While there may be no

malicious intent from these users to the enterprise, the lack of required expertise and dedicated IT resources can compromise the confidentiality, availability, or integrity of a KMS. Never-the-less, there is a business requirement to allow remote access to KMS.

Private - Internet (P-I)

The Private-Internet intersection is a concern, because it is with this realm that other entities can share the firmôs data over the Internet and other extranet connections. Because they are distinct external networks, it may be difficult, if not impossible to detect data loss in this space. The Private-Internet intersection is primarily a concern because of the role it plays as a host for threats from the Internet and as an infection vector for mobile enterprise assets to be exposed to unpatched and infected machines. Just a few seconds on an unprotected home network can be enough to compromise an enterprise client. Additionally, data stolen or leaked from the KMS may be traded in the P-I without our knowledge. More concerning still is the potential for data leakage from the Enterprise by devices that move freely between P-E and P-I-E zones (smart phones, flash drives, iPods, etc).

Private - Internet - Enterprise (P-I-E)

Devices that connect to the enterprise networks that have previously connected to either the Internet or private networks can be infected. Stafford and Urbaczewski (2004) outline some of the many internal threats such as spyware and adware. From an infection standpoint, it does not matter where the infection originates, the internal networked devices are compromised. The greatest potential threat of all the threats described in the P-E is a direct connection to the Internet. The recent US Department of Transportation (DOT) case is a prime example of this. The teenage daughter installed Limewire on her motherôs DOT laptop. The result was that sensitive DOT documents were then shared across the Internet. Spyware that is often part of a peer to peer application can also send usernames and passwords in addition to data from the Enterprise out to the Internet. When this occurs, Enterprise security administrators having no way to monitor or react to those threats.

Aside from active embedded threats, loss of portable computing devices represents another external threat. The Veterans Administration is a prime example of information being lost into the Internet and Private realms. In May of 2006, a laptop containing personnel records of 26.5 million veterans and active military was lost. Additionally, the VA reported in January of 2007, up to 1.8 million records stored on a portable hard drive were lost or stolen. Once this information is lost, there is no way to track where it goes or who uses the information. The only effective means to prevent the loss in the beginning is with effective controls in place. Maureen Regan, counselor to the VAôs Inspector General, stated that as of March 2007, the VA still lacked the effective controls needed.

Enterprise - Internet (E-I)

The Enterprise - Internet zone is where traditional Enterprise Information Security resources have been focused: firewalls, intrusion detection technologies, data leakage monitoring systems, proxy servers, etc. Outward facing resources within the Enterprise are usually relatively secure, there are ever increasing numbers of regulations and requirements that focus on securing this segment, and are increasingly more prescriptive, e.g. PCI and HIPAA. As evidence of the relative success of the efforts to secure resources in this zone, the emergence of threats in the other zones ï if it was easy to inappropriately access Enterprise resources the new threats wouldnôt take the long way around and attack by passing through private networks of remote workers and business partners.

Impacts for KMS

Organizations need to consider the threats from all these various realms to their KMS and what they would / will do when the data is compromised, traded, and sold across the Internet and Private networks that are beyond our control. Solutions such as drive encryption for data at rest inside and outside the organization for all devices that touch the KMS should be employed. The data in transit (or in motion) should be encrypted as well to ensure that capturing or *sniffing* of legible data cannot occur. While protecting data at rest and data in transit is a good start, it is not enough. Organizations that employ KMSs should enforce secure passwords that go beyond just password complexity and move to passphrases so that passwords are not easily bypassed by guessing, brute force analysis, or rainbow tables. While many organizations have employed some of all of these solutions, they are not employed consistently throughout the enterprise. Every device that can touch the KMS must be viewed as a potential unauthorized entry point to the KMS. This includes home machines, mobile devices such as smart phones and tablets, as well as web portals and workstations inside the organization.

Summary

In the years since the initial analysis the threats enumerated by the PIE model have only become more pronounced. With the relatively new phenomena of the ñconsumerizationò of many enterprises, traditional controls and management approaches are no longer possible. How does the firm ensure timely patch management or that only authorized software is installed when the enterprise doesn't own or manage the device? While some organizations have boldly moved into a Bring Your Own Technology (BYOT) model by heavily leveraging virtualization approaches and web 2.0 technologies, the threats identified within the PIE model and by the lack of consistently applied controls, available audit trails, and the murkiness of application of eDiscovery requirements to personally owned devices only adds to the confusion.

As was stated in the initial analysis, a KMS has numerous threats from the private, internet, and enterprise realms and their intersections that must be addressed. While there is no panacea for safeguarding a KMS, we believe that using the PIE model aids in raising the awareness and recognition of the different threat vectors that exist. The model also recognizes that these same areas of potential threat are also the areas that frequently provide value to the organization and are consequently a necessity. Ubiquitous connectivity and increasingly powerful personal

mobile computing devices are potentially both a blessing and a curse. Anywhere , 24x7 access to information assets means that staff can be far more productive than just a few years ago, but it also means that security teams have far less control over the assets they are charged with protecting.

References

Antonopoulos, A. M. (2004). New Data Center Strategies Newsletter. http://www.networkworld.com/newsletters/datacenter/2004/0531datacenter1.html [On-line].

Kaplin, D. (2011). DigiNotar breach fallout widens as more details emerge. http://www.scmagazineus.com/diginotar-breach-fallout-widens-as-more-details-emerge/article/211349/ [On-line].

Koger, M. S. Information Security Breach Disclosure: When, How Much, and To Whom. The ISSA Journal. January 2010.

Koger, M. S., & Landry, B. J. L. (2010) Personal mobile computing devices - the new perimeter. Association of Business Information Systems (ABIS), Dallas, TX.

Landry, B. J. L., Koger, M. S., Blanke, S. J., & Nielsen, P. C. (2009) Using the Private-Internet-Enterprise (PIE) model to examine IT risks and threats due to porous perimeters*, Information Security Journal: A Global Perspective.* 18, 163-169.

Landry, B. J. L. & Payne, D. (2006). Technical perspectives of illegal Peer-To-Peer (P2P) file sharing: Technical solutions are available. *International Journal of Services and Standards, 2,* 228-237.

Oltsik, J. (2011). RSA Reveals More Details About Its Security Breach. http://www.networkworld.com/community/blog/rsa-reveals-more-details-about-its-security-b [On-line].

Stafford, T. F. & Urbaczewski, A. (2004). Spyware: The ghost in the machine. *CAIS, 14,* 291-306.