Securing the Enterprise

Cyber Security Myths and Reality

"Machine learning, endpoint containment technology, dynamic behavior analysis", these are just some of the features promoted by endpoint protection products today.[1] "Deep packet inspection, anomaly based detection, stateful protocol analysis" are features promoted by intrusion detection and protection systems. All of these technologies promise wonderful results, but remember that while cyber security effectiveness is difficult to measure, promises based on new technologies are easy to make. Implementing real cyber security should be based on security controls founded on the analysis of actual successful breaches. This paper will discuss some well known recent security breaches, how they occurred and some recommended cyber security controls which would have prevented these breaches. We will also discuss some common cyber security myths and why the recommended security controls are a practical and effective solution for cyber security.

[1] "Magic Quadrant for Endpoint Protection Platforms", Gartner 30 January 2017

The Breaches

US Office of Personnel Management (OPM)

The OPM breach was first publicly announced in early June 2015. The summary results were that a likely nation-state was persistent on the OPM network for almost one year and absconded with about 20 million detailed security clearance records of US government employees and contractors. In addition the attackers absconded with 4 million personnel records and 5 million fingerprint images of US government employees.[2] The impact of this breach was severe. The agency director resigned and the CIO took early retirement. There were comments made that intelligence personnel were removed from some overseas posts.

How did this attack happen and why was it not discovered earlier? There is no public official analysis of this attack, but there are some important facts and clues which have been made public. First why did it take so long to discover the breach? After all the US civilian federal government agencies have spent $billions on an intrusion detection and protection system (IDS/IPS) called Einstein. It turns out that Einstein was not updated with the latest signature files, but even if it was, the traffic from the installed malware was encrypted so Einstein would not have been able to inspect this. It took a dedicated security staff person to manually decrypt the traffic and notice some beacon like signals to a domain not part of OMB, opmsecurity.org. That domain is now off limits to federal systems, but how difficult is it for an attacker to create a new domain?

Would encrypting the data have helped? Not in the case of the OPM breach. Once the attackers gained a foothold onto the OPM network, they were able to discover and use elevated user privileges which allowed them access to the data whether it was encrypted or not. But two factor authentication would have prevented access to the stolen data. In the case of the US government this means that a physical smart card must be used in addition to a password to access the network.[3]

Would an endpoint protection system with behavior analysis and machine learning, have prevented the breach? Maybe but this technology would not have been a requirement because the attack relied on known vulnera-

---

[2] "Inside the Cyberattack That Shocked the US Government", Wired 10/23/2106.

[3] ABOUT PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS, NIST.

bilities, not on an unknown "zero day" vulnerability. Curt Dukes, formerly chief of the NSA IAD (Information Assurance Directorate) gave an excellent interview explaining that none of the civilian federal government breaches that IAD was recently involved with relied on zero day vulnerabilities. This included the OPM, IRS, White House (EOP) and Department of State breaches.[4]

This last fact has some pretty major implications. It implies that organizations should first focus their security efforts on good cyber hygiene, i.e. applying software updates and security patches to operating systems and applications. Once they have a process which continuously monitors the endpoints and keeps them up to date, then they might consider technologies that help with zero day vulnerabilities. However since zero day vulnerabilities are rarely used in practice, possible mitigations against these vulnerabilities should be a low priority.

Adobe source code

In October 2013 Adobe acknowledged that source code for its ColdFusion Web application suite and for its Adobe Reader products were stolen. This source code would give the perpetrators great insight into possible vulnerabilities on a product such as Acrobat Reader which is installed on most end user computers throughout the world.

On his Krebsonsecurity blog, Brian Krebs states that Adobe acknowledged that the attackers appear to have gotten their foot in the door through "some type of out-of-date" software.[5] It would be poor irony if the out of date software was Adobe ColdFusion.

San Francisco Metropolitan Transit Agency (SFMTA)

SFMTA was affected by a ransomware attack on November 25, 2016, and was forced to allow customers to ride for free until their systems could be restored from backups. The cause of the breach was an un-patched Oracle Weblogic server(s).[6] The patch was released by Oracle a year earlier.

---

[4] Defending cyberspace: A report from the front with NSA Deputy National Manager for National Security Systems Curt Dukes, October 18, 2016 interview at the American Enterprise Institute.

[5] Adobe To Announce Source Code, Customer Data Breach, Krebs on Security, 03 Oct 2013

[6] Muni system hacker hit others by scanning for year-old Java vulnerability, Ars Technia, 11/29/2016.

Fortuitously the perpetrator's email account was hacked and security investigators found that this same attack was used successfully against a number of construction and manufacturing firms in the US.

Lesson learned - put a high priority on keeping publicly facing web servers up to date. They can be easily scanned for out of date and vulnerable software.

Ukrainian Power Grid

On December 23, 2015 the Ukrainian Power Grid experienced outages to about 225,000 customers. Fortunately the outages only lasted a few hours, but it was determined that the outages were caused by infiltrated IT and SCADA systems at the Ukrainian Power Grid companies.[7] A thorough analysis of this breach was performed by SANS based on publicly available information. In addition the report offers lessons learned.

This breach used email spearphishing to deliver Microsoft Office (Excel or Word) documents with a macro that when run installed the malware.[8] Once the attackers gained a foothold in the IT network, they were able to escalate user privileges, scan the network to discover VPN connections and hide their presence on the network. The attackers were also able to access the SCADA[9] system controlling the power sub-stations and thereby shutting down the system six months after they first gained access to the IT network.

Recommendations to prevent similar breaches would be to implement desktop computer configurations such as the US Government Configuration Baseline (USGCB) or the Center for Internet Security's Benchmarks (CIS Benchmarks). While these benchmarks would prevent the Microsoft Office macros from running on the desktop computers, they can also cause issues for normal use of these machines. Another recommendation is to regularly analyze all incoming and outgoing network traffic for suspicious behavior. Because only small amounts of data were taken, these malicious data packets were probably few and infrequent, so they may

---

[7] Analysis of the Cyber Attack on the Ukrainian Power Grid, SANS & Electricity - Information Sharing and Analysis Center, March 18, 2016

[8] "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents", Secure List January 28, 2016.

[9] SCADA (Supervisory Control and Data Acquisition) systems are often general purpose computers running Microsoft Windows desktop or embedded operating systems. Wikipedia "SCADA".

have been difficult for an IDS/IPS system to automatically discover. Hopefully this technology will improve in the future to help make this task more automated.

The Myths

Prioritize securing high value assets

If my organization's valuable data is only located on a few servers, why not just focus on securing those servers and data?

As we have seen from the breach examples above and in many other cases, the initial breach is often on desktops with no direct access to the high value severs and data. The attackers are then able to escalate or find user permissions that enable them access to the high valued systems and data. Simply patching the high value servers, encrypting the data or using Data Loss Protection (DLP) systems would have made little impact on preventing these breaches.

End point protection (EPP)

Won't our new EPP system automatically stop attacks using known and unknown (zero day) vulnerabilities? We just invested a lot of money in a new EPP system that uses behavioral analysis, machine learning, application containment, among other features. They promise to be able to stop zero day attacks. Why should we prioritize installing patches for known vulnerabilities?

Zero day vulnerabilities are very rarely used in cyber attacks. Even the high profile attacks on the US federal government described above (OPM, White House, IRS, Department of State) were all based on known vulnerabilities. Verizon's 2016 Data Breach Investigations Report only mentions one zero day vulnerability used in a breach.[10] Therefore prioritizing protection against zero days attacks does not make a lot of sense.

Installing patches and software updates is a big effort in most organizations. However since these known vulnerabilities are often used in successful breaches, do you really want to count on some un-proven technologies such as behavioral analysis and machine learning to stop these attacks? It seems a wiser choice to patch and update the organization's IT systems. See a discussion of the CIS controls in a later section of this paper.

[10] Verizon Data Breach Investigations Report 2016

IDS/IPS will stop most attacks

Our new IDS/IPS system offers features like deep packet inspection, anomaly based detection, stateful protocol analysis. Why won't that identify and prevent any breaches of our IT network?

An IDS/IPS may be useful in discovering that a breach has occurred, but there are a number of issues with these systems that you should be aware of before relying on them too heavily. As we have seen in the US government breaches described earlier, if the IDS/IPS system is dependent on attack signatures and those signatures are not updated or are unknown, then the IDS/IPS will not identify or prevent a breach.

If the attack involves encrypted data packets then the IDS/IPS system will be less likely to identify that a breach has occurred. If the network address used in the attack packets is faked then the IDS/IPS will be unlikely to identify the attack or that a successful breach has occurred.

Focus on critical vulnerabilities

Patching and updating applications and operating systems is very manpower intensive and time consuming. Wouldn't it make sense for us to focus on the critical (high CVSS) vulnerabilities?[11]

The NIST NVD CVSS scores are a measure of the ability to use and the impact of a known vulnerability. It would seem to make a lot of sense to focus on the critical vulnerabilities, i.e. those with high CVSS scores. Unfortunately attackers look at these CVSS scores too and the majority of vulnerabilities used are those with CVSS scores lower than critical.[12] The lesson is clear that all vulnerabilities need to be remediated, not just the critical ones.

Focus on recent vulnerabilities

Since it's hard to install all of the needed patches, wouldn't it make sense to focus on just recent vulnerabilities?

Attackers continue to use old vulnerabilities as long as they work. You can clearly see this in Verizon's 2016 DBIR report, Figure 12, where the vulnerabilities published as CVEs in 2015 account for less then eight percent of the total vulnerabilities actually exploited in 2015. In fact the largest number of vulnerabilities exploited in 2015 were initially published as CVEs in

---

[11] "The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities." NIST NVD CVSS.

[12] "A Preliminary Analysis of Vulnerability Scores for Attacks in Wild - The EKITS and SYM Datasets"

2007! [13] This implies that organizations need to update their systems for all vulnerabilities, no matter the CVSS score or the date of the vulnerability.

Realizing that it's very difficult to remediate for all vulnerabilities, Gartner has an interesting proposal.[14] Since less than ten percent of total vulnerabilities were actually used in malware, focus on remediating those vulnerabilities.[15] This makes a lot of sense as an initial priority, however there is nothing to stop the attackers from using other vulnerabilities on short notice. In fact Gartner's report shows that from 2014 to 2015 the number of vulnerabilities used in malware increased by 50 percent, so you would need to keep close tabs on which vulnerabilities are being used.

Two factor authentication

Isn't two factor authentication overkill and maybe just for US Department of Defense users? I can cover this control by managing what my users can access and encrypting my sensitive data.

As we have seen from the breach examples above, many attacks are able to find or elevate user privileges. If only passwords are used to access sensitive data, then even if this data is encrypted, there is a strong likelihood that the attackers will either find or create authorized user accounts and access the sensitive data. The best way to prevent this is to require usage of two factor authentication on all user accounts. It is also important to have a system which will automatically track changes to user account privileges and usage throughout the organization.

Isolated networks

Why do we need to secure our isolated networks, such as our industrial control system (ICS) or SIPRNet[16] system? By definition they are isolated from our regular network and from the public Internet.

These networks are not always as isolated as advertised. Industrial Control Systems are often managed by SCADA systems, which may or may not

---

[13] Verizon's 2016 Data Breach Investigations Report.

[14] "It's Time to Align Your Vulnerability Management Priorities With the Biggest Threats", Gartner 9 September 2016

[15] In 2015 there were 807 exploited vulnerabilities and 8,243 not exploited vulnerabilities, per the Gartner paper referenced above.

[16] SIPRNet (Secret IP Routed Network) used by the US Department of Defense and other federal agencies. Wikipedia.

have outside connections. As we saw with the Ukrainian Power Grid, the SCADA systems had VPN connections which the attackers were able to take advantage of. There have been instances within the US military where compromised USB storage devices were able to breach the SIPR-Net. These breaches on isolated networks show that the same security controls should be applied to these sensitive networks that apply to our regular networks.

The Recommendations

The CIS foundational controls

At Belarc we try to keep things simple, so here's our recommendation on how best to implement cyber security: Establish a process to implement and regularly monitor the Center for Internet Security (CIS) Foundational Controls. We like the CIS controls because they are based on lessons learned from actual attacks and breaches and are created by people from multiple industries and government, including the NSA and DHS, who have deep knowledge of all aspects of cyber security.

This is from the CIS:

"The CIS Critical Security Controls (CIS Controls) are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks. The CIS Controls are developed, refined, and validated by a community of leading experts from around the world. Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent. Implementing all 20 CIS Controls increases the risk reduction to around 94 percent."

In total there are only twenty controls and the first five are what the CIS calls foundational. Here is a summary listing. Please download the CIS Controls document for a full description of the controls.

- CSC 1: Inventory of Authorized and Unauthorized Devices.
- CSC 2: Inventory of Authorized and Unauthorized Software.
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges.

The CIS Controls document also lists a mapping to the NIST Framework for Improving Critical Infrastructure Cybersecurity and a section on creating Security Governance Controls targeted to senior management and the organization's board of directors.

How Belarc can help

Belarc's system automatically creates an up to date central repository with detailed hardware, software and security configuration data. It does this on a near continuous basis and scales to enterprises of any size. See architecture discussion in the following section.

Maps to the CIS foundational controls

Belarc's capabilities map very closely to the CIS foundational controls, as follows:

- Complete listing of all hardware including desktops, laptops, servers, virtual machines, tablets and phones. Configuration details include make, model, serial number, BIOS or UEFI, operating system, group policies applied, USB storage device usage, encryption status, and more. CSC 1.
- Complete listing of all installed software including versions and last time used. Ability to automatically compare installed software with standard images or approved software. Flags unused software as candidates to be removed. CSC 2.
- Comparison of configurations to the US Government Configuration Baselines (USGCB). CSC 3.
- Automatic vulnerability assessment based on published vulnerabilities from Microsoft, Adobe, Oracle Java and Apple. CSC 4.
- Detailed information on both local and domain user logins by host and privileges, and the ability to automatically track user account changes such as elevated privileges. CSC 5.

Belarc's Intranet Cloud architecture

Belarc's system was designed to operate over the enterprise's Intranet Cloud, either on premises or SaaS. Belarc's Cloud architecture is based on lightweight data gathering agents which use the enterprise's Intranet and

requires only one server and a single database (see Figure 1 below). The agents communicate directly with a single Belarc server via https (SSL/TLS) protocols, avoiding the need for a hierarchy of servers or scanners and replicating databases. Users can access the data via secure two factor Web browser authentication, based on a need to know.

Allows for rapid deployment and low maintenance

Belarc's Cloud architecture allows for rapid and easy system roll out and extremely low ongoing maintenance. This is because there is no need to install and maintain local servers, scanners and databases. Belarc's products also use the existing TCP/IP network and standard protocols, so that there is no need to manage special router settings across our customer's network. There are also substantial automation features built into Belarc's products which eliminate the need for the manual efforts required by other systems.

Ideal for tracking mobile devices

Mobile devices are becoming ever more useful and pervasive in today's enterprises. Belarc's Cloud based architecture is ideally suited for mobile devices because these devices natively use the Cloud to communicate with the enterprise's IT resources. For example, when remote laptops or phones connect to the enterprise network, Belarc's client will automatically upload their profiles to the enterprise's Belarc server. No additional infrastructure or setup is required.

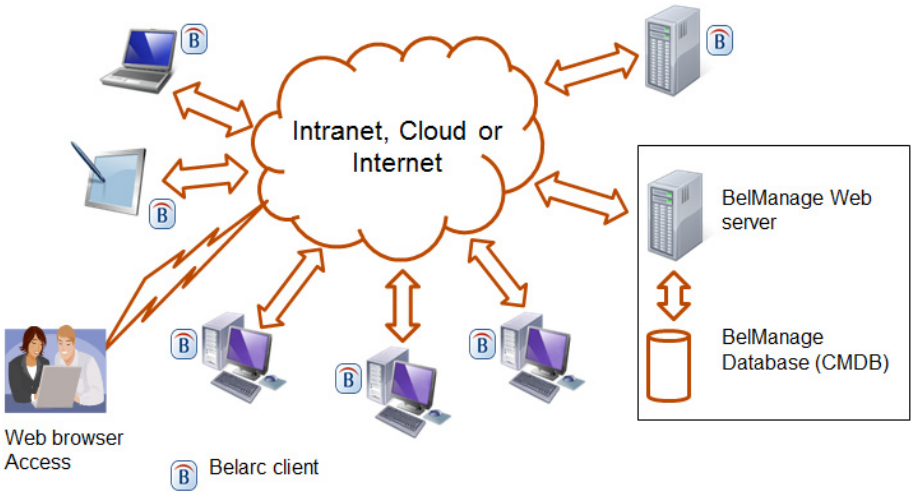

FIGURE 1. Belarc's Cloud architecture

Central repository of configuration data

Another major benefit of Belarc's Cloud architecture is that it automatically creates a central repository, or Configuration Management Database (CMDB) consisting of detailed software, hardware and security configurations. Belarc's CMDB is automatically updated, usually on a daily basis, with accurate and complete information. This obviates the need for gathering data from multiple sources as with a federated CMDB approach.

Proof Positive

Belarc's products have been successfully used by thousands of both small and large enterprise customers for over sixteen years. Brief descriptions of how some of our customers are using Belarc's products are described below.

Texas Department of Transportation (TxDOT)

The Texas Department of Transportation deployed Belarc's SaaS system on 16,000 IT assets, including desktops, laptops, servers, virtual machines and phones. Belarc's agents covered all of their Windows, Linux, and iOS operating systems. The profiles are uploaded to a SaaS server on an hourly basis and reports are rebuilt daily. TxDOT uses both the standard BelManage web interface and Belarc's powerful Data Analytics module to help them correlate the vulnerabilities with past breaches and to help remediate the vulnerabilities.

US Federal Aviation Administration (FAA)

The US FAA deployed Belarc throughout their enterprise on over 57,000 IT assets in under one month. Their initial justification for Belarc was for software license management and the system has already helped the FAA identify over $million in un-used Microsoft desktop software. Belarc's data also allowed the FAA to effectively negotiate a $tens of millions overage request from IBM. Belarc's system is also being used in their Microsoft EA true up, including desktop and server software, Oracle database software, IBM, Adobe, ESRI (ArcGIS), and other high value software agreements. As a by-product of the data Belarc's system collects, it is also being used to track many of the NIST 800-53 security controls, and the Major Applications for the Portfolio Management process.

USAF 844th CG

The USAF 844th CG, covering over 25,000 IT assets at the Pentagon JCS and Joint Bases Bolling and Andrews, has been using Belarc's system since 2007 for managing their enterprise software license agreements and to monitor their security controls. BelManage was initially used to offer authoritative data for their Microsoft EA license true-up, resulting in a $2.7 million annual savings on this ELA alone. It was submitted as for a

Best Practices Nomination. In addition Belarc is used to help monitor the USAF's vulnerability status and other security controls.

Kindred Healthcare

Kindred Healthcare is one of the largest healthcare providers in the US with over 300 hospitals and nursing homes in 28 states. Kindred has been using BelManage since 2002 for software license management on over 25,000 of their servers, desktops and laptops located throughout the US. Local administrators and HQ personnel log into their BelManage system on a daily basis for both operational, security auditing and software licensing and purchasing tasks. Kindred manages their BelManage system with a fraction of an FTE.

Catholic Relief Services (CRS)

CRS is located in 101 countries on five continents, offering humanitarian services. Their BelManage system runs on 5,000 clients often located in very remote areas and updates are sent to their BelManage server when connections are possible. Their BelManage system is used for ITAM, SLM, configuration control and IT security.

Summary

There are lots of interesting new technologies being applied to cyber security, particularly in end point protection and IDS/IPS products. Some of this may become helpful in the future, however when we analyze actual security breaches it is clear that to achieve real security the organization needs to follow good IT practices. This can be accomplished by implementing and continuously monitoring simple but proven security controls from organizations such as the Center for Internet Security. Belarc's system is ideally suited to accomplish this in an automated and low cost fashion.

Contact Us:

For additional information please contact us:

Belarc Benelux
(ITAMSoft B.V.)
Den Ilp 8
1127PA DEN ILP (Amsterdam)
Tel: +31 (0)20 - 4822603
Email: info@belarc.nl
Web: http://www.belarc.nl

Contact Us: