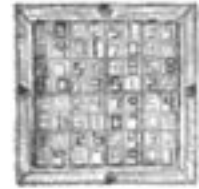


CONTENT MANAGEMENT SECURITY: TREAT YOUR SYSTEMS LIKE YOUR HOME

ADAM RESNICK, *Cipher Systems*



Successful organizations are systematic in their approach to sending market signals. For example, they time press releases strategically, keep critical data confidential, and deliberately launch products with both customer and competitor *windows of opportunity* in mind. These organizations understand the value of the knowledge created within the firm – their intellectual property – and go to great lengths to protect it. In this column I will share some of the secrets of firms who successfully secure their electronic content management systems.

A content management system (CMS) is a collaborative application for managing documents and other information sources. In many environments today these systems are web based and provide secure access 24x7. Systems may include advanced search, indexing, integrated workflow, document versioning, image management, and other features. Typically the system is installed internally but it may be hosted by a third party. In all cases security and user management is a high priority.

In many respects, securing a CMS is similar to how homeowners secure their homes. Both often use the following techniques:

- Lock the doors to prevent outsiders from coming in.
- Install intrusion detectors inside the home to detect individuals inside.
- Don't leave the front-door key under the welcome mat.
- Store valuables in a home safe.
- Leave copies of irreplaceable papers inside a safe deposit box.

Each of these common-sense techniques makes it harder for a hacker

to break in. (A hacker is defined as anyone who abuses technology. Abusing technology in itself is not considered good or bad; it is simply a collection of techniques used to achieve a goal. That goal may be to disrupt a company (e.g., destroying an email server) or to snoop around an organization's network undetected.)

The more defenses you employ, the more difficult you make it for the intruder.

LOCK THE DOORS

Most web-based CMS require users to login with a combination of username and password. They are the equivalent of your front door lock. Most CMS builders expect users to enter only through the front door.

The better CMS come equipped with a more heavy duty lock: Secure Socket Layer (SSL). The SSL protocol encrypts everything sent between the web user and the web server. At a minimum, you want the usernames and passwords entered by users to be encrypted over your networks. In other words, make sure your front door has a good lock.

The back door, however, is often left unlocked. As software vendors become aware of break-ins and other hacking attempts, they release patches and updates – the equivalent of locking the back door. Although often time-consuming, applying patches on a regular basis goes a long way towards preventing hackers from exploiting holes in your CMS.

In addition, know who is accessing your CMS database. Carefully monitor user accounts; the fewer accounts the better. Actively review your user access list and lock or remove any unused database accounts. If you accidentally

remove someone who legitimately needs access, they will let you know. You are better off being proactive so that it is easier to identify unwanted system intruders.

Web applications are entered through a web server that is running either inside (intranet) or outside (extranet) of a firewall. Do not assume that your intranet is adequately secure just because it is running behind a firewall. You will need to employ additional security tactics in addition to the firewall. Otherwise you are making your intranet site particularly vulnerable and you risk the exposure of the particularly sensitive information that resides on your intranet. In fact, extranets tend to be more secure than intranets, so more hackers tend to target intranet sites directly.

ADD A SECOND LAYER OF DEFENSE: INSTALL MOTION DETECTORS

Some homes also have motion detectors installed inside key entranceways. Homeowners who have these detectors understand a critical weakness about locks: thieves can often get around them if they try hard enough. The motion detectors provide a second layer of defense. To secure your content management system, you want the equivalent of an internal motion detector – an Intrusion Detection System (IDS).

Intrusion Detection Systems come in several varieties. There are open-source, freely available IDS (e.g., Snort, <http://www.snort.org/>) and proprietary products. They all perform the same job: to automatically investigate network activity and report any irregular patterns.

Online actions like roaming a network, using a web server, writing documents and others all leave computer trails in the form of packets sent over the network. An IDS will examine packets, looking for unusual behavior – e.g., ports that are rarely used, logins at unusual times, etc.

Actively monitor your system for unexpected activity. For example, if your system is accessed only during regular business hours, watch for system use outside of these hours. You should also write automated programs that alert you to file changes. Check file sizes and file modification dates on files and directories periodically. If a directory size changes by a byte (and the files are static), then you've been tampered with.

The critical point is to have systems in place that alert you to unusual activity. Don't expect your system and network administrators to spend time going through log files one line at a time, looking for unusual activity. There are simply too many logs generated from the normally enormous amounts of activity these content management systems generate. Instead, use automated systems (such as IDS) to examine the logs for you.

DON'T LEAVE THE FRONT DOOR KEY UNDER THE DOORMAT

Although the doormat may seem a convenient place to "hide" your key, it is the first place a thief will look. The equivalent concept in content management security is allowing your CMS administrators to share or reveal their passwords. Or worse, your users fall prey to social hijackers who call or email people in your organization and trick them into revealing their usernames and passwords.

To prevent this kind of behavior, the organization needs to institute policies. Have clear consequences for this kind of sloppy security such as fines or even dismissal. The behavior of system administrators is often guided by past examples. If they are aware of other administrators who were

known to share passwords but were not punished they may see this behavior as acceptable. If there are immediate and

Identify unexpected user activity.

public consequences when a system administrator is caught sharing his password, others will work much closer within your security guidelines.

Similarly, have positive incentives for maintaining tight security. For example, have bonuses for ensuring that passwords stay secret and strong (e.g., incorporating the appropriate complex mix of letters, numbers, and punctuation). Also have incentives for reporting security violations.

STORES VALUABLES IN A HOME SAFE

If you had a \$50,000 necklace at home, you'd keep that valuable asset in a heavy duty home safe. When it comes to content management systems, the valuable assets are your database and static files.

To protect static files, reduce permissions to the absolute minimum. Ensure that these files are protected by anti-virus software. And make sure that your operating system (whether Windows, Unix, Mac, or Linux) has the latest security patches applied. Although applying patches is time consuming (and expensive), they do contain critical security fixes that you do not want to operate without.

To protect your databases, make sure that the latest security patches are applied (e.g., Oracle actually schedules patches to its flagship database product on a regular basis throughout the year). Minimize the number of database accounts that exist. A typical content management system will employ two types of database accounts: an owner and a user account. The owner account

is used to create the database. Once the database has been established, this high-powered account should be locked tight. You should be equally vigilant when managing your user accounts. When users leave the company, please close or lock the unused accounts. By carefully managing database accounts, you reduce the number of entry points into your database system.

Just as you wouldn't leave that \$50,000 necklace sitting on the kitchen table, you shouldn't leave sensitive competitive intelligence information sitting on your computer or on an unsecured department server. Instead, store it on a server that is in a secure space with limited access.

Think about your setup today: can anyone walk into the space where your critical data servers are located? Or, do they need a special ID badge that keeps track of who entered the room? Simply asking users to write their names on a sign-up sheet before entering a restricted server room sounds like a good idea at first but it gives a false sense of security. After a while no one looks at the sign-up sheet. I know of friends that signed the name Indiana Jones on the sign-up sheet for weeks at one large organization before anyone noticed. And, even worse, once someone noticed, several meetings were held, and no changes were instituted. If you are going to create an access log, at a minimum, make sure those who enter present a valid photo ID. Using badges and card-readers that automatically record time and identity upon entrance and exit is even better. Then there is a digital record of who arrived and when.

USE A SAFETY DEPOSIT BOX

A will provides directions for what to do upon a person's death. Many homeowners keep a copy of their will (along with other irreplaceable papers, wedding picture negatives, etc.) in a safe deposit box at the local bank. This ensures that in the event there is a fire and both the home and its owner are

destroyed, there are written instructions left at a separate location providing next steps. Thus, the homeowner prepares for the worst case scenario and has setup instructions for what to do going forward.

To secure your CMS from the ultimate disaster, you need your own version of this safe deposit box: an offsite backup of your CMS data along with detailed instructions listing how to restore it from scratch. It is not unreasonable to expect your building to be damaged through a storm, flood, or fire. When this happens, your servers will be dead and you will need to rebuild your system from scratch. It is in these moments that you will be grateful you created an offsite backup. To remain effective, this offsite backup must be kept up to date on a regular basis (at least once per quarter).

For the individual or smaller CI department, if you want an easy way to protect your valuable files, here's a tip: purchase a portable USB hard drive. You can find these at most computer and office supply stores. This hard drive stays off and locked-up most of the time (to keep it out of reach from hackers and to make it last longer). About once a month turn on that hard drive, connect it to your computer or department server, drag and drop all of your valuable files to it, and then turn it off. Finally, lock it in your desk drawer or remove it to a secure offsite location. Hackers cannot get to it. If your computer crashes, your valuables are protected.

Many organizations do a wonderful job of creating backup tapes, but how often do they actually test them to make sure they can bring the system back? Not often. You need to write down, step by step, how to rebuild your competitive information from nothing. Simply, imagine you bought new servers and had to start over: what do you need to recover? Answer that question first, then test the answer, document it, and put in your safe deposit box.

content management systems become increasingly complex, it becomes easier to break into them. If you wish to secure your CMS, employ the same common-sense techniques used by millions of homeowners today. With each additional layer of protection, you make it that much harder for a hacker to break-in. If a hacker can access critical servers, then that hacker can most definitely look inside your computer, read your emails, and access your crucial files.

No system is 100% secure. If someone wants to break into your home, they will. Likewise, you need insurance against unexpected disasters. You must

When did you last back up your files?

not only try to prevent hackers, but you must be prepared for the possibility of your system's destruction.

Look for security solutions in the real world. For example, the police cannot be everywhere at once and yet automated red-light cameras have been very effective in reducing the number of people who are running red lights. Similarly, intrusion detection systems (IDS) do just that – watching firewall logs and network packets for the unusual, etc. Using IDS and other forms of automated watchdogs increase the odds of detecting intruders once they've stepped inside your home.

Use common sense. Don't put a heavy duty lock on a paper door. It does not matter how many tactics you employ to secure your system if the point of access is given away. Make sure your system administrators are not giving out their passwords to others and that users are not sharing their own. Keep in mind that a lot of sensitive information is kept on department servers and desktops, so employees need to be held accountable at all levels.

Put a strict security policy in place and make sure that there are

clear consequences to violations. Again, think in terms of real world expectations. If I rob a bank and I'm caught, I'll probably go to jail. Likewise, if a user creates a password that would be obvious to hackers, or shares it with others, a punishment should be applied and advertised to the rest of your department or organization. Finally, be wary. Most hackers find users quite willing to give their usernames and passwords over the phone or in response to email requests – do not give this information out under any circumstances.

The basic principles of electronic content management security are partially physically-driven and partially technology-driven. They are all underlined by common sense. Following the tips outlined in this article will help you better protect your electronic assets and ensure they are kept out of the hands of your competitors.

Adam Resnick is a senior consultant at Cipher Systems (www.cipher-sys.com). Cipher specializes in competitive intelligence consulting and technology services for both the public and private sectors. Services include primary / secondary data collection, analysis, reporting, company profiling and scenario planning. Cipher's award-winning CI software Knowledge Works is a customizable toolkit of CI technologies. Adam can be reached at a.resnick@cipher-sys.com or (410) 451-6889.

CONCLUSION