FIRING A NETWORK SECURITY ADMINISTRATOR – BEST PRACTICES

Firing any employee can be a stressful event. Firing one who has significant knowledge of and privileged access to your Information Technology/Security infrastructure is even more stressful, as the risks are so notable:

- Administrative access to critical business systems and data
- Destruction of data
- Theft of confidential data
- Publication of confidential data
- Web defacement or disruption
- Email disruption
- Physical access by terminated employee
- Emailing malicious content to susceptible users
- Network access disruption
- Third Party Service Provider Relationships/Access
- Administrative Access to key Web Assets / Information (Domain registrars, web-based services)

We have outlined some good practices for dealing with the dismissal or resignation of a key IT/IS employee to reduce these risks. The greater risk this employee and situation pose – the more of these practices you will need to execute.

PRE-FIRING ACTIVITIES

- Conduct a network/system level vulnerability assessment/penetration test to determine where you might be vulnerable externally. If your risk profile is high, it would be better to augment the VA/PT with a security architecture review to provide a higher level of assurance.
- Understand what systems are external to your organization for which the user may have privileged access: hosted web sites, ISP routers, exposed administrative interfaces on firewalls, DR sites, PBX interfaces. User account reviews and changing of administrative level passwords post-firing are likely necessary. Be aware that system to system communication may leverage these passwords and that some things may "break" if you don't map these dependencies before making the changes.
- War dial or perform a telecommunication audit to ensure that you have accounted for all POTS lines. A good security architecture is easily defeated by a back-door modem. Remember, many mainframes and SANs have modem support lines for DR purposes.
- War walk or conduct a wireless security audit to ensure that your WLAN is properly authenticating users, is not visible from public locations outside your buildings, is using an appropriately strong encryption scheme, and doesn't contain any "rogue" access points, which again can be leveraged as a back door to defeat even the best security architectures.
- Ensure that all remote access mechanisms – VPN, Citrix, Terminal Services, and Dial-up modems/RAS are secure. Determine if local authentication takes place at any of these points (as post-firing you will need to disable the employee's accounts), do a review/clean-up of all accounts, and force a password change.
- Ensure that your physical security measures are sufficient to protect against unauthorized malicious entry. Try tailgating, validate that security guards check badges, and observe whether delivery personnel are granted access to areas where they should not be. It is common that we can compromise physical security with very simple social engineering tactics like these.
- Validate that you have backups of critical files/applications/configuration so that systems can be restored if necessary.
- Search Social Networks (LinkedIn, Facebook, MySpace, etc.) for your company's name. Although not a direct threat to your data's confidentiality, integrity or availability, the former employee might have noted his employment there. This is a good thing to do regardless if there are any pending layoffs or firings.

DURING FIRING

- De-provision access to all systems possible just prior to notifying the individual. (Remove all administrative access)
- Provide a severance package that spaces payment over several months and cites that the severance is based on their cooperation and good behavior. This is generally a very effective deterrent.
- Ensure that all assets: phones, PDA's, laptops, credit cards, keys, access cards, and tokens are retrieved and tracked.
- Do not immediately "re-issue" the laptop. Preferably, store it in a secure manner or take a forensic copy of the hard-drive if any suspicious, inappropriate, or criminal activity was suspected. Recently, the forensic copy was useful for a client when they were sued by the ex-employee. On review it was determined that the individual had forwarded dozens of confidential company documents to their home email address prior to leaving. The company counter-sued the employee and eventually won the case. Some companies will review the activities over the previous month or so to determine if the user had accessed sensitive data in anticipation of leaving.
- If the user enjoys administrative access to many systems, before their termination, have them continually observed while they work with a highly trusted individual who will acquire and change passwords for every critical system. We have seen too many instances where a network admin has been fired and escorted out of the building and only after the fact was it discovered that there were systems for which he, alone, knew the admin password.
- Notify all personnel immediately that the person is no longer an employee and that any communication with the individual needs to be reported to management.
- Notify all consultants, vendors, and business partners immediately that the person is no longer an employee and that any communication with the individual needs to be reported to management. One of our clients did not take this step and the fired employees had a consultant pull business critical data from a database and send it to his home email address. The ex-employee explained he was working from home and was having "VPN problems" so the consultant (not knowing the person had been fired two days prior) exported the data and sent it him. This was only discovered after the ex-employee sold the data and a poison pill in the data notified the company.

POST FIRING

- Remove all ex-employee administrative access.
- Change company domain account password with domain name vendors. Change the technical administrative contact if necessary.
- Ghost laptop and make copy of all shares with critical data.
- Change voice mail password.
- Continue to de-provision access to all systems possible. Obvious points are Primary Authentication Servers, mail servers, file/print servers. However, there are often many local authentication points – WLAN, servers, business applications, network devices. For all high risk areas consider a user account review clean-up, and force password changes for all accounts, especially any "shared" administrator accounts.
- Force a password change for all employees (it is not uncommon for an admin to know other peoples' passwords).
- For all critical systems (remote access, key applications, firewalls, etc.) validate that logging is enabled and working properly and monitor the logs for a period of time to detect any rogue access attempts.
- Leverage your IDS and/or outbound firewall rules/logging to detect any Trojans installed by the employee that may communicate outbound.
- Return to the previously identified Social Networks and ensure that there have not been any disparaging or false comments made about you (if you are the ex-employee's boss) or a principal of the company or the company itself. While this is not a direct threat to your data per se, disparaging and false information could damage you and your company's reputations.

The **GREATER RISK** this employee and situation pose – the **MORE** of these practices you will **NEED TO EXECUTE.**