5525 Green Bay Road
Kenosha, WI 53144-3737

PARTNERS, L.L.C.
Certified Public Accountants
and Consultants

Telephone: 262/657-2060
Fax: 262/657-2080
www.ppgpartners.net

Ten Tips for Reducing Insider Security Threats

(By Scott Matteson) Insider threats can pose greater risks to company data than those associated with external attacks. Some insider security breaches can go undetected for weeks, months or years.

Here are some techniques to help you spot and mitigate them as quickly as possible.

1. Establish a security incident and response team.

Even if it consists of one individual, a dedicated team is essential to security success. This team should be responsible for preventing, detecting and handling incidents and have documented plans and procedures for each. Providing them, as well as general IT staff, with security training to keep up on the latest tactics and threats is also a key factor in identifying insider threats as quickly as possible.

2. Use temporary accounts.

Set up third-party employees such as contractors or interns with temporary accounts which expire on a certain date, tied to the end of their contract or project. This will ensure the accounts are inaccessible after the individual departs.

3. Conduct frequent audits to look for unused accounts and disable or remove them if possible.

A simple use of the "dsquery" command on a Windows Active Directory Domain Controller can do the trick.

4. Follow employee termination principles carefully.

Remove access and disable accounts as soon as possible when staff departs. HR and employee managers should be in direct contact with IT when employees leave or there is a plan for them to do so. Many financial companies alert IT staff in advance of planned terminations so the former employee's access can literally be shut off as they are being walked out the door.

5. Identify unhappy employees.

Disgruntled employees may be more liable to pose as insider threats out of a desire for revenge, a plan to steal data, or simple greed combined with lack of respect for the organization. Not only should these employees be monitored, but you should also make an effort to alleviate the source of their unhappiness, if possible, to improve the situation.

- Continued on Page 2 -

Get daily updates and relevant news alerts by following us on Social Media!

Connect with PPG Partners Online!

twitter.com/**PPGPartners**

facebook.com/**PPGPartners**

linkedin.com/**company/ppg-partners-llc**

- Continued from Page 1 -

6. Use two-factor authentication.

Often described as "something you have and something you know," the most common example is the use of an RSA token which displays a rotating sequence of numbers that consists of an authentication code. Users need to type a password or PIN followed by this ever-changing code to gain access to a system, so anyone who obtains either the password or the token (but not both, obviously) will be blocked at the gate, as it were.

7. Use encryption of confidential data either in motion or at rest.

This one is straightforward; encrypt data using whatever software or hardware technology fits the bill, and make sure to use this as it is stored or traveling over a network. That way if someone is capturing traffic, steals a hard drive from a server, or gets their hands on a backup tape they won't be able to get to the data involved.

8. Consider third-party products.

One type of product which can help is an identity access management solution, which can help manage the provisioning and de-provisioning of identities, access, and privileges, and assist in managing the authentication and authorization of individual users within or across system and enterprise boundaries.

Data loss prevention and user activity monitoring are also referenced in the ICIT report as two more key solutions to help reduce insider risks.

A product like “Tripwire” can also be useful here. Tripwire monitors systems and notifies you when any element on them changes, such as a password file, a confidential spreadsheet, or an SSH key.

Now, many files can and do change each day, so there may be a high signal to noise ratio at first, but you should be able to filter out normal activity from abnormal activity after establishing baseline patterns of activity to detect suspicious behavior.

9. Don't forget to guard your perimeter.

You may recall the movie *When a Stranger Calls*. That was the film whereby a babysitter kept receiving threatening phone calls and had the police trace them, then was told, "We've traced the call...it's coming from inside the house!" You might argue that this was the ultimate insider threat, but keep in mind the villain had to have gotten in somehow. Don't assume you have to only guard the interior of your network; focus your security initiatives and efforts upon all external-facing devices as well.

10. Consider investments in products and staff more than just "insurance."

This is really more of a mindset than an action item, but it's worth discussing. Too many executives seem to think security products are just mindless insurance they have to pay for or else something bad might happen. That's the wrong approach and can lead to grumbling over budgets. Certainly we don't view policeman as a drain upon a town budget, especially when we need their help.

Good security practices can also reduce scrutiny (or penalties) from auditors for certain institutions. And it's important to keep in mind that spending a little (or a lot) on security can help prevent much larger costs down the road, such as lost revenue in the wake of a data breach.