for those who seek brilliance

Interacting with End Users re: Security

How to Strike the Balance between Security and Convenience for the "Normal" User

Adam Haeder
Vice President of Information Technology, AIM

The job of a security professional

"PROTECT THE NETWORK" - Confidentiality, Integrity and Availability

- **Confidentiality**: let the 'good' people have access to the data, prevent the 'bad' people from accessing the data
  - Authentication methods - Who are you? And can you prove it?
  - Authorization (or Control) methods - What can you access?
- **Integrity**: Is the data itself 'good'? Has it been changed? When and by whom?
- **Availability**: Is the data available per the company's requirements (which are usually 24/7 and from any device on the planet)? Who accessed the data? With whom did they share it?

AIM

The job of a knowledge worker

"USE THE NETWORK" - Create, Modify, Access, Transmit data

- **Create**: Make something out of nothing
- **Modify**: Change data
- **Access**: Examine data
- **Transmit**: Share data

AIM

What we expect of end users

- Different passwords for everything
- No sharing of account credentials
- No re-use of passwords
- No movement of data outside the network
- No non-approved devices on the network
- Restricted access to personal data/sites from the corporate network
- No non-approved software on the network
- Questioning "new" people or processes

AIM

Situations - Passwords

- **Employee needs access to data to which they don't have access.**
  - SP solution: employee requests access from supervisor, supervisor fills out change form, SP gets assigned the task, SP completes the task, SP notifies the user
  - Employee solution: Use another employee's login to access the data OR call someone with access and ask them for the data

Who is right?

AIM

Situations - Passwords

- **Employee is required by policy to change their password every 90 days.**
  - SP solution: employee changes their password every 90 days to something completely different, with no connection to the last password
  - Employee solution: husker123 -> husker234 -> husker345 -> husker456 etc....

Who is right?

Situations - Passwords

- **Small company uses 4 different "cloud hosted" apps with no single sign-on. How do employees manage their passwords?**
  - SP solution: employee creates different passwords for each app and voluntarily changes them every 90 days (or whatever the policy says)
  - Employee solution: Same password on every account OR password_quickbooks & password_email & password_foo

Who is right?

AIM

Situations - Moving Data out of the network

- **Employee wants to run queries on a large data set, but lacks the local CPU power.**
  - SP solution: employee needs to work with internal IT to find storage space and cpu time in the existing company infrastructure
  - Employee solution: Upload data to an Amazon EC2 instance, run the queries, download the results.

Who is right?

AIM

Situations - BYOD

- **Employee needs access to a site for research purposes that runs some NSFW ads, making the whole site blocked by the corporate firewall.**
  - SP solution: employee needs to put in a formal request to whitelist the site
  - Employee solution: bring in personal tablet, access site over 3G

Who is right?

AIM

Situations - Non-approved devices on the network

- **Employee needs to test development websites on a mobile browser, company disagrees, so no mobile testing is done.**
  - SP solution: employee needs to follow the chain of command, request a change to the formal testing process, and have the company purchase mobile devices to use as test stations.
  - Employee solution: bring in personal tablet, connect to company wifi, run the tests

Who is right?

AIM

Situations - Restricted access to personal websites

- **Employee tasked with raising awareness about upcoming product launch, wants to create a Facebook page, facebook.com blocked at work.**
  - SP solution: employee needs request that facebook.com be unblocked either company wide or for her workstation for a defined time period.
  - Employee solution: Create the page on personal phone with Facebook app OR connect to facebook.com through an anonymous proxy.

Who is right?

Situations - Non-approved software

- **Employee wants to use the Gimp for simple image editing, but it's not on the 'approved' list.**
  - SP solution: employee needs to request that the Gimp be added to the "officially approved" desktop software list
  - Employee solution: Install it myself.

Who is right?

AIM

Situations - Non-approved software

- **Company policy mandates Internet Explorer 7 as the only approved browser. Employee needs access to sites that don't work in IE7.**
  - SP solution: employee needs to lobby the company to change the policy
  - Employee solution: Install Chrome, access the sites.

Who is right?

AIM

Situations - Security Personnel

- **A new employee shows up at Bob's desk and says that a virus has been detected and his machine needs to be cleaned IMMEDIATELY.**
  - SP solution: Bob should verify the employee's credentials before giving him access to anything, perhaps by calling a supervisor
  - Employee solution: "Yet another IT issue", gives the employee full access to his computer (still logged in as 'bob'), goes to get a coffee.

Who is right?

AIM

Common Themes

From the perspective of the security professional:

All instances required the employee to take some specific action

From the perspective of the employee:

All instances amounted to ways to slow the employee down. Preferred solutions often involved doing something yourself, rather than going through 'official' channels.

Questions

What is the average employee's reaction to security policies? Why?

What is the average security professional's reaction to the average employee? Why?

AIM

Take aways

Try and see if from the employee's perspective - above all else, they just want to get their job done.

IT is supposed to consist of tools that allow an employee to get their job done MORE efficiently.

We (as IT professionals) are supposed to facilitate this connection of tools to employees. Even when the employee acts like a tool :)

AIM

Password Managers

- Application - Device
  - LastPass
  - KeePass
  - Universal Password Manager
- Application - Web
  - phpPasswordManager
  - Web-KeePass
  - phpPassSafe
- Home Grown
  - GPG + text file
  - GPG + text file + Dropbox
  - GPG + MySQL

for those who seek brilliance

Adam Haeder
Vice President of Information Technology
ahaeder@aimforbrilliance.org

@adamhaeder

www.aimforbrilliance.org