ACME Scandinavia - Secure IT Environment

Review of Analysis and System Design

February 20, 2015

Analysis and System Design made by Group 5

Review made by Group 1

Adam Johansson *Erik Norell* *Ignacio Quezada* Cruz *Micke Söderqvist*

EP2520 - Building Networked Systems Security (BNSS)

Strong points

- Using a VPN in tunnel mode between Stockholm and the London branch seems like a good (and natural) solution. We notice that type of encryption is not stated, SSL/TLS/ipsec? Additionally, you do not state whether you want to use transport mode tunnel mode.
- Using an internal CA and digital certificates to authenticate users is also a good solution.
- The design of the two factor authentication (2FA) meets the requirements as far as we can see.
- A firewall is included as well which is of course necessary to stop outsiders from entering the network. It is not stated how the firewall will warn if attacks are detected, by logging? Email?

Weak points

- We notice that WPA2/PSK is used for authentication of users for the WLAN. We are a bit concerned about security using this option. There is no mentioning of a scheme for changing passwords or strength of password (is it hard to remember? Strength in terms of dictionary attacks?) as it is stated. Even with that addressed there is a risk of the password leaking to unauthorized users.
- The need of an intrusion detection system has not been addressed.
- The current solution for file transfer between mobile phones doesn't actually permit file transfers. It grants read access to employee's public folders on the web server which is not quite the same. You can for example not send a file to a single recipient, every employee can read the public folder of another employee.
- We noticed that only WLAN has been mentioned. Does this mean that Ethernet will not be used for the desktop computers? It is stated that non-laptop users will have to use 2FA to authenticate themselves, does this include desktop computers as well? Mobile phones? Is it necessary?

Suggestions for improvements

- Digital certificates are already in place with the current design, so authentication of wireless users could be done using WPA2 Enterprise instead. It would increase security in this aspect as well as better integrate with the current proposed design.

- Perhaps not an improvement per se, but a reconsideration of design. As there is already a PKI in place you could use HTTPS and 2FA for users outside of the network. It would achieve security and grant access to the webserver. It is not required that users have full access to the internal network from home, only the web server. Perhaps this has already been considered as an option but rejected for reasons not mentioned here?

- Perhaps state how ACME is supposed to revoke and create new certificates.