Dan Wnuk
DSS
1/25/2012

Article Summary 3

This article opens with a paragraph describing how Fortune 100 companies are routinely attacked and compromised nowadays, and it has become common knowledge. What people do n't realize, however, is that home users are targeted equally as often. The article describes how mission-critical systems are often "dual-used", that is - they are used for the critical tasks, but also used for things such as checking email or Facebook, which the article deems as entertainment tasks. Security is not taken seriously by a vast majority of users - the article states that security sometimes gets in the way, i.e. preventing a user from doing something that could be malicious. The user, instead of thinking better, gets around this security block. An example I can think of would be turning off a firewall to play a videogame, or use something like a file sharing program. If the firewall is blocking the user, then the user will simply turn it off, but that opens them up to a whole slew of possible attacks. The article brings up the question of how we keep a computer secure while also allowing users to bypass it when something critical is happening. The article then brings up probably one of the points that I find scary - the possibility for an ISP to monitor users' activity, with the goal of helping and guiding them. While this could be beneficial to newer users, if this were put in place it would massively raise privacy issues. If the ISPs are able to see all of our data, what is going to prevent people from stealing that data, or from law enforcement forcing that data over to them? This is all too real with the recent SOPA and PIPA legislation in Congress, and it is something that I take very seriously. Another topic that is covered in the article is the idea of cloud computing, and whether or not it will aide in stopping this whole insecurity mess or if it will only amplify it. On one hand, I could see it creating more of a problem because now all of your data is elsewhere and you can't even physically control it. It is really up to the company to protect it, and why should you be trusting anyone else with your critical data? On the flip side, however, you no longer have the dual-use of the system going on. In cloud computing, the servers are all stored in some data center, so no one will be logging in to Facebook or opening a virus from their email. There really are two sides to that issue, and I'm not sure which one I would lean more towards. I think cloud computing is a good step in the right direction, at least for startups, because they no longer need to buy a server room and host their own sites, they can simply pay a small(ish) monthly fee depending on activity.

In general, this article does a very good job of summarizing the current state of security

(or lack thereof), as well as the typical actions performed by a user (shutting off the firewall if it is blocking you from doing something). It is very broad but briefly touches on a lot of key issues that I find interesting: security, security in cloud computing and potential methods to increase security. Security is my application domain, and I'm passionate about coming up with new ways to keep everything secure. The information from this article will help with my software development because it made me realize that no one is safe from attackers, and it is often the fault of the people using the system. The current knowledge of these problems, and the ability to point them out, are essential to creating even better security. While I don't think that having ISPs monitor users activity to help them is the correct step, there are likely certain methods that remain to be seen which could make things exponentially more secure. The only real question is when will we find out, and will it be too late?

Article Information

Title: Living with Insecurity
Authors: William Arbaugh and Deborah A. Frincke
Obtained from: http://www.computer.org/portal/web/csdl/abs/mags/sp/2011/06/msp201106toc.htm