written by Thomas Maroulis on 20 December 2016 in devops, engineering

security, mind your entry-points

This is the first in a new series of posts where we are going to be covering security best practices, one bit at a time. The field of software security can be extremely broad and complex so to keep things simple (and to keep strictly within the limits of what I feel qualified to talk about) we are going to keep the format simple and only talk about one topic at a time.

Without further ado...

It seemed fitting to start at the outermost layer of infrastructure and set things off by talking about entry-points or more formally about perimeter security.

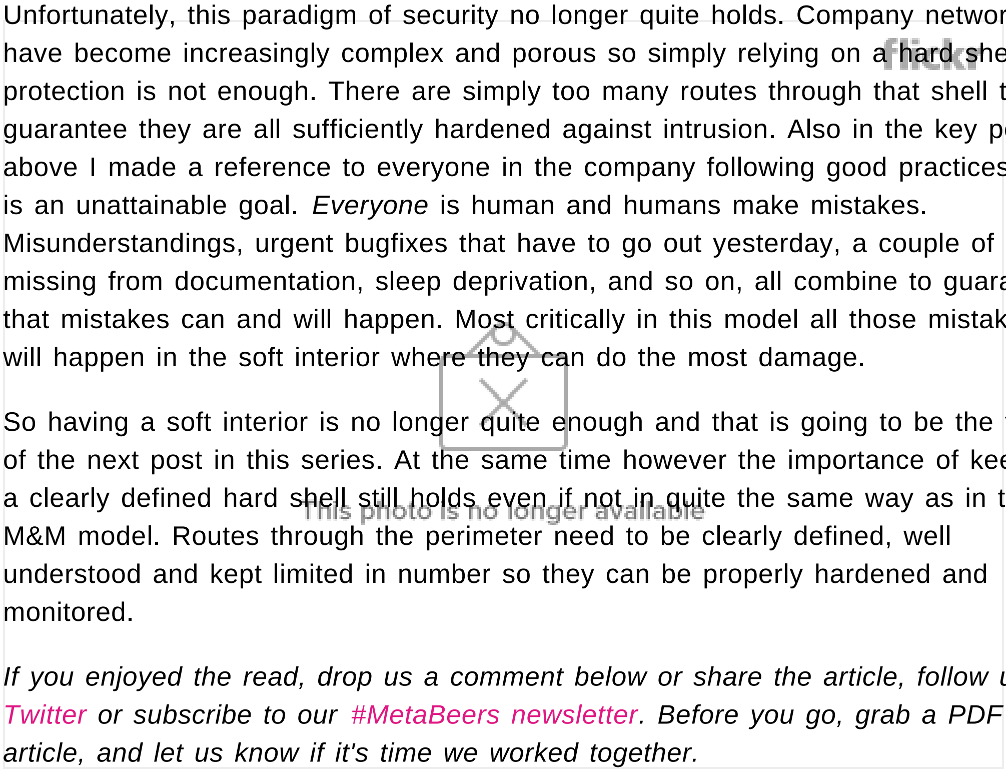
walls for the information age

The traditional way of viewing security is as an M&M. A hard shell that conceals a soft interior. The idea behind this is simple.

- The network outside our walls is outside our control and therefore dangerous
- The network inside our walls is under our control and therefore with a good security design, good day to day practices and good training to ensure everyone in the company understands and follows these practices it can be made safe

On the face of it this makes sense. After all defending against threats is a complex and difficult problem so if we can limit the surface area that we have to defend by providing only a few clearly defined *gates* through our perimeter we can make our job easier.

At the same time security is often a tradeoff between itself and usability. If the internal network that employees will spend most of their time accessing is cumbersome to use then people are sure to find *creative* solutions to work around it.



Unfortunately, this paradigm of security no longer quite holds. Company networks have become increasingly complex and porous so simply relying on a hard shell for protection is not enough. There are simply too many routes through that shell to guarantee they are all sufficiently hardened against intrusion. Also in the key points above I made a reference to everyone in the company following good practices. That is an unattainable goal. *Everyone* is human and humans make mistakes. Misunderstandings, urgent bugfixes that have to go out yesterday, a couple of lines missing from documentation, sleep deprivation, and so on, all combine to guarantee that mistakes can and will happen. Most critically in this model all those mistakes will happen in the soft interior where they can do the most damage.

So having a soft interior is no longer quite enough and that is going to be the topic of the next post in this series. At the same time however the importance of keeping a clearly defined hard shell still holds even if not in quite the same way as in the M&M model. Routes through the perimeter need to be clearly defined, well understood and kept limited in number so they can be properly hardened and monitored.

If you enjoyed the read, drop us a comment below or share the article, follow us on Twitter or subscribe to our #MetaBeers newsletter. Before you go, grab a PDF of the article, and let us know if it's time we worked together.