PRINCIPLES OF DEFENSE - GENERAL GUIDELINES

Defending your IT infrastructure is a tricky and time consuming business, and there are many different details to bear in mind, depending as well on type and size of your IT infrastructure. But, no matter what size or technology or type of business you are involved in protecting, there are some general rules to keep in mind when working out the details. I cannot claim to have originated, or to being the author of these guidelines, some are commonly known principles, some are common sense, but regardless, I have found them to be true enough time and again.

- *The "Outrun-the-Bear" Defense*
  We all know the joke (and if you have'nt, you will now) about the two friends walking in the woods and they stumble across a large, grumpy and hungry bear. When the one man gets ready to run, his friend tells him that it is useless as a bear can easily outrun a man. To which his mate responds "I don't have to outrun the bear, just you." This is the most basic rule of your IT defense, deal with the fact that there is no perfect, un-hackable defense, but you can secure your infrastructure so that attackers will rather try someplace easier, or realise that the effort and risks involved are not worth the probable rewards.

- *Enforce the concept of "Least Privilege"*
  Almost all attacks happen through the breaking of some trust relationship. Whether its a server-to-server trust, or a trusted employee, or a trusted client, or any other situation, it is the breaking of these trusts which enable attacks. This can be limited if in setting up your IT infrastructure, you make sure to give any resource only what is needed to fufill it's function. Nothing more, nothing less. This could be applied to the rights of users on a network, all the way to only running the required services on a server. By only giving what is needed, you limit the damage which could be caused by an attacker exploiting a trust relationship.

- *Make your first answer "No"*
  Everything that is and will happen on your IT infrastructure can be classified in three ways 1) Something Good, 2) Something Bad, and 3) Not Sure. Simple right? You see, dealing with the first two is easy, it is the third type which causes most of the problems. If your stance is only to stop things once they are proven bad, then you fall prey to those things which have not yet -for whatever reason- been proven bad yet, but actually are. But if you only allow those things that have been proven good, then such "grey areas" will hold no threat, as anything new has to prove itself good before it is allowed. This way of thinking is nothing new to those who administer firewalls, or even to those who approve new medicines.

- *There are such things as "Weak Links"*
  This is similar to the trust relationship principle. But this deals with the fact that -no matter what- there will be weak links somewhere in your infrastructure. They could be an employee with a legimately large amount of authority, or a server that has to run an unsecure service (against your recommendations of course). These will happen, these will be targets for attackers, and these are your weak links. What you must do to recognise this and therefore increase your monitoring of these weak links and endevour to make them as secure as possible under the circumstances.

- *Have a "Not-a-Smartie" Network*
  In case you don't know, Smarties are small discus-shaped sweets. They have a thin outside coating of candy, underneath this is chocolate. When it comes to snacks I like smarties, but as a blueprint for an IT infrastructure the idea .. sucks. If your infrastructure is all "crunchy" on the outside (firewalls, proxies, etc) but yet inside your network you are using exploitable versions of software, insecure protocols, bad passwords, etc. You then have a "Smartie" network, crunchy on the outside, but soft on the inside. You need to have "Defense-in-Depth". This entails multiple layers of defense/protection. If you have multiple layers of defense protecting your infrastructure than any attacker has to work that much harder, and it lessens the chances of a single attack causing a wide level of access. Such layers could include VPN's, secure protocols, proper passwords, proxies, multiple firewalls, etc.

- *Realise that Variety is good*
  Similar to "Defense-in-Depth", is the principle of "Defense-in-Breadth". What this means is that if your infrastructure is protected by only one type or make of defense, then it really does'nt matter how many times you've layered them, one exploit will still fit all. It makes better sense to have similar defenses but from different sources, this way if a defense from source A has a certain exploit, you'll still be okay because the same defense from source B does'nt. Think of it a an automated second opinion. An easy example could be to have a dual layer of firewalls, each from a different vendor, each supporting the others weak areas.

- *Make sure that all Access is through Chokepoints*
  Try as much as possible to limit all access to your infrastructure or highly sensitive assests is restricited to coming through one -or as close to one as possible- points. For example your internet access should all go through one firewall, your email should all come through one gateway server, etc. restricting access or data flows to such chokepoints offers serveral benefits. The most important of which is that you can better monitor and secure them. It also makes it more economical in concentrating your resources, as you know which are your most important channels.

- *Enable the "Fog-of-War"*
  Security through obscurity is a concept which has received a fair amount of negative publicity. Much of this is well-deserved. As a first and last line of defense, using security through obscurity is a recipie for disaster. But as a single principle in an already well setup infrastructure it makes a lot of sense. The simple principle is that you should make the attacker work for every last thing they want. Why make their jobs any easier by having public DNS information? or easily accessible corporate phone lists? Heck, you spent long enough setting your infrastructure up securely, let them suffer.

- *Keep It Simple ....*
  However much we may not like it, we are human. And to err is human. When setting up your infrastructure try to keep things simple, not unsecure, just simple. By limiting as far as possible the complicated setups on your infrastructure you make maintainence easier, as well as the monitoring of your infrastructure. Most importantly you lessen the chances that you would have made a mistake. There will be times when you have to have something complicated in your infrastructure, but always remember that true genius is being able to make complicated things simple.

- *Watch your Infrastructure*
  Finally, as a general principle and also to be used in conjunction with all the above, make sure that you know what is happening on your infrastructure. Monitor it, read the logs, establish baselines, find out what is happening and why, be pro-active in checking new events and fixing any possible avenues for exploit. Make sure that you don't only do something because the famous human by-product has hit the fan. Do not shirk your responsiblities.

Always remember that these are guidelines, and it is entirely feasible that you may need to setup an IT infrastructure in an environment where some of these are just not possible. But keeping these in mind in whatever you do should help