Taking it to the bad guys in 2016

Ian Trump returns to the front line of cybercrime prevention with some solid advice on how to keep your clients safe in the coming year.

Turning your corporate network into a strategic Anti-Access/Area Denial (A2/AD) zone is a long-term task for anyone running up against cybercriminals – and let's face itthat means anyone with a network. The military defines an A2/AD strategy as a secure 'bubble' that is achieved by using layered defensive systems. Failure of a single layer should not relinquish the battle space, and by battle space I mean your corporate assets. Make no mistake, in 2016 your customers' corporate assets will be on the front line of the battle space. To be successful in maintaining control of them you will have to deploy technology, improve process and implement policy.

To exert control in the contested space, a mixture of both defensive and offensive tactics will be required. Ultimately, your goal is to construct concentric rings of defence that increase the 'cost' for the cybercriminal to gain access. In this struggle your philosophy must change from guarding the physical assets to understanding the data, its importance to the business operations of your client and ultimately where it exists in the network and how protected it is.

Deter cybercriminal targeting

The first defensive ring has a lot to do with business and employee online presence. The best approach to take here is to educate users through security awareness training. Be upfront about what data is important to the business and tie that to a confidentiality policy. Social media monitoring is useful to help employees make good decisions about what to share outside the company. The goal here is to look at violations of these policies as learning opportunities – unless the violation is malicious or so egregious that it requires management action. Weekly vulnerability scanning is a great way to minimise business risk, by helping you understand when you have to move fast to close up defensive gaps.

Disrupt cybercriminal tactics

Cybercriminals looking to break into a system with malware will invariably turn to phishing attacks, using malware attachments or web links. Technology is central to this part of the defence and works well with the user awareness training previously mentioned. Removal of administrative privileges, mail protection, web protection and aggressive patch management are the key elements needed to prevent infection by malware. The first three levels try to knock out the threat before it reaches the end-points; if it makes it past these measures then patch management comes into play to ensure there is no vulnerability available to exploit. Keeping systems up-to-date and maintaining a small attack surface raises the cost for cybercriminals, and this forces them to resort to rare and expensive zero-day attacks.

Degrade cybercriminal capability

Once cybercriminals have made it inside an organization, the key is to detect and respond to their activity as soon as possible. Robust antivirus, event log checks, network monitoring and daily backup are the key technologies of this defensive layer. Many organisations re-image machines if any indications of compromise are detected. In a well managed network environment, a machine exhibiting activity such as transmission to a foreign IP address(es) is identified and investigated. In the case of a ransomware attack, disinfection of the infected-endpoint and restoration of the encrypted files from backup is the best route to take. Having to pay a ransom means you are not doing a good enough job for your customer.

Destroy cybercriminal infrastructure

It would be awesome if defenders like us had access to drones and cyber weapons to strike back at the bad guys; unfortunately we don't. However, there are things we can do to the bad guys that can take away some of their infrastructure. These include, making a complaint to the hosting ISP, hosting company, domain registrar or any piece of the infrastructure that is being used in an attack against you or your customers. If you have access to legal counsel and the attack was serious it may also be worth a letter to all involved and notification to law enforcement. Since the Internet is essentially one big neighbourhood, subscribing to a threat intel feed to block IP addresses of attackers can win one for the good guys. Maybe your security failure can help someone else. After all, we are all on the Internet together.

A balanced, layered defence is an effective way to keep your customers or business safe, and there are lots of great products and services on the market that augment user awareness training. If you want to know more about how to justify a layered approach to your clients, then check out this blog: Are you set for the war on your data in 2016? Ultimately, the more rings of defence you can create, the more chances you have to avoid or detect a system compromise.

Ian Trump is security lead at LOGiCnow

You can follow Ian on Twitter at @phat_hobbit

Ian Trump

Security Lead at LOGICnow
Ian Trump, CD, CPM, BA, is an ITIL certified Information Technology (IT) consultant with 20 years' experience in IT security. From 1989 to 1992, Ian served with the Canadian Forces (CF), Military Intelligence Branch; in 2002, he joined the CF MP Reserves and retired as a

Public Affairs Officer in 2013. His previous contract was managing IT projects for the Canadian Museum of Human Rights. Currently, Ian is the Security Lead at LOGICnow working across all lines of business to define, create and execute security solutions to promote a safe, secure Internet for businesses worldwide.