MSP Secure: Five Core Security Measures.

A friend of mine is very cognizant of the need for his business to implement good network security. And yet, when we discuss the mainstream technologies that should be protecting his network, and get to the pricing – he laughs at me! Well, he is a friend and can do that. But he is also my discipline. I read the newspaper and listen to the news, like everyone else. My jaw drops at the egregious network attacks, the data stolen, the impact – and the basic security measures that were not taken. This is the basis of our MTS – Secure offering, and is the focus of discussion in this white paper.

CTP has been speaking about network security for many years – the subject can be complicated and highly technical – we find we can lose our audience in a matter of moments! To keep things relevant, we look to i) convey that CTP, an MSP, also offers a Managed Services Secure service, priced moderately above the standard MSP offering; ii) provide very briefly, and without drama, an indication of how security may be compromised, and iii) list five security measures that we suggest are essential for every business network, followed by a reasonable amount of technical discussion – sufficient to make the presentation real.

MSP – Secure: a standard offering from Collaborative Technology Partners.

- *Managed Services Provider* (MSP): CTP a conventional MSP agreement that typically covers all computers and end-user support. This is a very commodity service, widely available and marketed. For a typical small company of a dozen people, cost tends to be on the order of $500 / month.
- *MSP – Secure*, a CTP offering that additionally covers core network security, is not currently a commodity service. CTP pricing for that same typical small company of a dozen people is on the order of $600 / month.
- The two price points mentioned make broad assumptions about the network and services involved – our intent is simply to indicate the relative difference in support cost for the scope of security services we identify in this white paper.
- There are many valuable and effective security solutions that may be implemented, and CTP loves to talk about them! But – they do not fit the scope of this presentation – what are the basic measures that every company should take.

There is an inherent problem with the topic at hand – it is hard to become motivated to invest in core security measures without understanding the problem – risks and counter measures – and yet the topic is arcane, technical, and too easy to dismiss as not relevant. We list three points to bring out relevance of this topic for Boston business, followed by five network security measures that are provided by our MTS – Secure offering.

1. With a user account and password, a hacker likely has ready access to your network. Those two things – username and password – are easily obtained via a variety of phishing techniques.
2. Today's hackers do not need to be technically knowledgeable – the attack tools are available on a SaaS basis – Software as a Service – hackers are simply purchasing services from a cloud service provider. This transforms the problem – hackers are now experts in your field of business – they are researching your company – the people, business, client base, resources and assets,

and then targeting their attack to individuals, drawing on very specific information behind the business of the company. Bear in mind that an attacker may initially develop information from compromised mail accounts of your customers, rather than breaches in your own network. That can give the attacker the specific information they need to select your business and begin to drill down, finding information directly engage your staff and partners, and insert themselves into your business processes.

3. Boston businesses in particular, and American businesses in general, are at significant risk of successful attack. Interest in Boston business expertise has been widely documented, and is global – countries through Asia and Europe, as well as domestic.

For a typical business in the Boston area, then, we have relatively easy access to the internal network, high motivation for attack, and elevation of highly sophisticated tools to the well-developed model of Software as a Service (SaaS), available on the darknet.

It is only prudent to take the view that the likelihood is high that your network will be compromised, and to turn attention now to how to most gracefully and transparently handle this reality. CTP lists five measures that are proven, effective, and should become as commonplace as the good Internet firewall that has already become standard best practice.

1. Two-factor authentication for all access to the network – PCs, remote access, and any other access to the network. Two-factor authentication is available both as cloud- and on-premises service, is highly effective and proven, and simply should be deployed by every business.
2. Web-reputation service – any web site may be attacked and compromised – entirely outside the control of your company. Any good anti-virus software and firewall security suite will protect your company based on web reputation, and both of these technologies should be engaged to work for you.
3. Compartmentalization. Every managed switch in common use for small business, and every good firewall supports virtual networking (vLAN), allowing for compartmentalization of your network – separation of end-user PCs from servers, management ports, VoIP, wireless, and perhaps Internet facing services. This topic is discussed further.
4. Account privileges. Accounts used to log into the end-user PC network should have only user privileges. There are good ways to provide access for all authorized people in your company to protected resources, while living with this rule of user only rights on the end-user PC network. Many problems are addressed by the disciplined enforcement of this simple policy.
5. Outbound connections to the Internet should be blocked by default. Firewalls are normally permitted to allow all outbound connections. With very few exceptions, no outbound connections should be required or allowed from any server, and the same is true for PCs.

There we are – five measures that make the CTP recommended core network security offering. Your business likely already owns all of the hardware and software required to support these measures. The two-factor authentication service might be the only exception, and it is available as a cloud-based service priced by user count.

You might notice that I have not included monitoring in this list of five core security measures. CTP thinks highly of monitoring, and of numerous other security measures – many sophisticated, effective and valuable. We love to speak to these topics, and routinely implement these for Boston companies. Our essential message here, though, is that these five security measures should be implemented by all companies. We know that many companies, even some of the largest companies, have not taken these measures – based upon the nature of the security breaches that are reported, and based upon our own experience as consultants.

It is likely that your company already owns the hardware and software necessary for implementation of these, aside from the two-factor authentication – but there is still the implementation part. That is where CTP comes in – we have the experience to implement these measures effectively and without locking your company staff out of your own network. We suggest that this is no small task – many years have gone into developing methodology behind these topics – and it is this expertise that allow us to offer secure MTS services at commodity pricing.

There were two topics among the five for which further discussion was promised: compartmentalization and account privileges. These relate to the case that your network has been successfully breached. For this situation, the hacker should be accessing your network via an account with minimal privileges, using a computer with no cached account information, and with no network access to protected company resources.

Compartmentalization – the concept that information and resources of similar sensitivity are grouped into individual security zones, limiting the access that a successful hacker has to the company network. An important tool for this purpose is the virtual LAN (VLAN) supported by most network switches and firewalls in use, even for a small company. Connections between network segments may be restricted to require authentication and inspection by the firewall, protecting servers and management ports of the firewall, switch and even printers.

Account privileges - the end-user account used on the PC should have only limited user rights, with no access to any other networks and no administrative access to the PC. There will be user access to a file share on the server, and rights to submit print jobs to the printer, but little else. An individual authorized to access network resources will have separate accounts for each security shell. The mechanisms are available within Windows to support this arrangement easily.

With these two measures, there is little the hacker can accomplish having gained access to the company network. They cannot, for instance, install software to the PC, as they do not have administrative rights to that PC.

This does not mean that there are no vulnerabilities – the hacker is free to copy the contents of the file share for which the end-user has access, to bundle that information up and transmit via a standard web connection to an external server, and in this way steal company information. This sort of activity can be detected – that is where monitoring comes in – both of the network and of content transmitted via the Internet. We know that many of our smaller customers are not sufficiently concerned about this sort of scenario to justify the expense of monitoring systems that are effective against this sort of attack. That is a business decision that will weigh knowledge of the specific content on the network of that company against risk of this sort of attack. Truthfully, for some companies there will be little or no content of concern on their network. And so we are satisfied with our recommended five core network security measures.