Topic:
Internet Security

iCT is produced by Business Advantage, a B2B research, business development and marketing consulting practice operating in the global IT, Digital and Telecommunication s sectors.

The Ultimate Blended Threat

Why is security failing in spite of all the technology available that is supposed to protect us against every theoretical threat that might possibly exist? Calum Macleod of Cyber Ark has a view.

Volkswagen Golfs and Baseball Caps

Calum Macleod – Western European Director for Cyber-Ark

A few days ago I became the innocent victim of a "blended threat" attack when a Volkswagen Golf and a Hyundai Getz joined together and rammed my two week old car sitting in front of my house. Of course as with all blended attacks it was impossible to foresee that an idiot in the Golf would drive at 70mph in a 30 zone and that my neighbour would decide to turn right into her driveway just in front of him with the result that they would blend together and target my car. And before you all start shouting women drivers, the police have decided that the moron driving the Golf was to blame. Like all Golf drivers he wears a baseball cap, sits at a 45 degree angle and the music blares out of the car to cover up the banging noise that usually comes from the gearbox. I love Golf drivers!

Worse was to follow when the fire department decided that the only way to get the neighbour, who wasn't seriously hurt apart from the wallop from the airbag – vicious things!! – was to cut the roof of her car. Of course size 16 boots and cutting gear on the boot and roof didn't enhance the appearance of my pride and joy. I'm still trying to find out who wears size 16 but they swear that they all do. If only I had parked in the driveway!

Now some of you might be wondering what on earth I'm talking about. What is a "blended threat"? According to the anti-virus folks this is "an attack combining a number of traditional attack methods, like a worm, a Trojan horse, and a keylogger", and like myself you might still not be any the wiser but it certainly sounds impressive. But the question is how susceptible are we to "blended threats", and are these the "blended threats" we really need to worry about.

Pel House, 35 Station Square, Petts Wood, Kent, BR5 1LZ, United Kingdom
Tel: +44 (0)1689 873636 **Email:** info@business-advantage.com **Web:** www.business-advantage.com

Today everybody, including your grandmother, is using the Internet and the vast majority live in a state of paranoia that everyone from Bin Laden to the taxman are attacking your PC every time they connect. However you would have to be increasingly unlucky – or parked in the wrong place – to fall victim to this and especially in the corporate world. Your IT security team has probably seen to it that you have every form of defence known to man on your infrastructure. In fact your PC is probably so well protected you can't even use it, and yet there is hardly a day that goes by that someone doesn't fall victim to another form of "blended threat". The key is that your IT security team are so focused on perimeter security and extended the perimeter to the end point that they have forgotten what they're supposed to be protecting, and equally importantly that the money to pay for frequently useless IT toys has to come from the business.

So why is security failing in spite of all this technology that is supposed to protect us against every theoretical threat that might possibly exist? Well probably because they're focusing on the wrong "blended threat".

The "blended threats" that pose the biggest risk are of a much more virulent strain than the odd virus or worm that finds its way to your PC. It's the "blended threat" of the dishonest employee who steals information from your business and the opportunistic taxman who is willing to pay him for it. Or it's the employee who used to work in the back office and now works as a trader on your banking floor. It could be the former IT employee who had privileged access to your systems and still has remote access, or the compliance officer who is being well rewarded for helping your competitor analyze your contracts. The biggest "blended threat" today is the worm you've hired to do a job and sets about to damage your business.

In a recent survey that Cyber-Ark conducted amongst 300 IT administrators, over a third admitted to using their privileged rights to access information that is confidential or sensitive by using the administrative passwords as a means of peeking at information that they are not privy to and snooping around the network!

Anyone who pays the slightest bit of attention, and hopefully your IT Security staff have, will be aware that the evidence has shown conclusively that up to 90% of incidents in business relating to the loss of assets results from staff that have privileged access to IT systems and applications. Another interesting side note from the study is that 57% who were responsible for the fraud should not have had authorized system access at the time of the attack. Some other minor stats that should not go unnoticed are that 81% of the organizations that are attacked experience a negative financial impact as a result of insider activities; 75% of the organizations experience some impact on their business operations, and 28% of the organizations experienced a negative impact to their reputations! I don't know of any worm, Trojan horse, keylogger, virus, or whatever else that can claim that level of success – unless a terrorized granny watching the news and believing that the latest computer virus will destroy world order in the next 24 hours!

Business Advantage
intelligence insight innovation

Pel House, 35 Station Square, Petts Wood, Kent, BR5 1LZ, United Kingdom
Tel: +44 (0)1689 873636 **Email:** info@business-advantage.com **Web:** www.business-advantage.com

If you want to deal with the real “blended threat” then protect your assets. This means that information that is essential to the life of your business is only accessible to those who need to get access to it. And if you think that this is all science fiction then let me share some of the requirements that I recently received from a company that understands what is of value. Among their requirements are

- End-to-end encryption of stored data and transmitted data.
- User-to-user information exchange via a secure digital vault.
- User-to-system or system-to-user information exchange. For example, automated systems processes to transfer files into the secure digital vault using a secure file transfer.
- Reduced need for manual intervention, facilities such as automatic email notification of files uploaded or retrieved.
- Secure tamper-proof audit trail that cannot be modified by IT personnel.
- Allowing information owners to control who can access their data in the secure digital vault, allow Audit to review who has accessed data without actually being able to see the data itself, and allow IT administrators to perform backups/restores/manage quotas without having visibility of the data itself.
- Provision of reports on secure activity, e.g. file uploads and retrievals, user creations and password changes, access right changes, failed authentication attempts, etc.
- Capabilities to limit the sources from which external users can access the data over the Internet.
- Provision of guaranteed delivery of large files, including resuming of partial downloads that were not completed due to network errors.

These requirements should be de-facto for any business, and it’s up to the business to take the lead and not continue to be dictated to by IT staff who don’t understand the business. As for me - I’ve decided the wife can park on the street. My car goes in the driveway from now on!

This article was provided by Calum Macleod, Western European Director, Cyber-Ark Software, Inc. For more information see www.cyber-ark.com or call +1-617-965-1544

Please Click HERE to leave a comment or question.