Productivity Enhancement and Protection
Improving Business IT Resilience
Graduated Benefits

2024-04-05

We understand that relatively recently a large Christchurch (NZ) Law Firm had its IT system made unusable for many days by computer malware.

On conventional business IT systems, by the time you detect signs of a breach it's almost certainly too late to prevent major operational flow disruption and big costs.

Unsurprising in view of some BigTech appearing to prefer charging you subscriptions for services to alert you to problems happening instead of eliminating the problems.

Microsoft's annual income from 'security' subscriptions now exceeds USD 20 billion, and yet the plague of malware outbreaks on Windows-based business IT systems continues apparently unabated. As security expert Kevin Beaumont has commented “Microsoft is the world leader in monetising its failure”.

When malware invades business IT systems almost all of them rapidly get every server and every desktop disabled.

The situation has been likened to having a sudden heart attack followed by needing open-heart surgery.

The full effects of sudden blood or data flow disruption are grossly underestimated by most. Problems can easily persist for months.

Maintaining operational flow is what really matters, and we can deliver that for you.

Our approach is unique in that we expect malware to invade a business's IT system. But the business continues running regardless, due to the benefits of the technology and techniques we provide that keep operational data flowing.

We also provide flexibility. You decide how much benefit to get, and how much downtime there'll be when malware invades.

Imagine how comfortable you and the rest of your staff will feel once you all know how little effect a Windows malware outbreak will have with our stuff in play.

There's currently 3 categories of client for our Business IT Resilience Improvement components. Enquire for details : https://iopen.co.nz/ws_contact.html

The following are the major components of our approach :

Using Virtual Machines

Typically businesses have MS-Windows installed directly on machines. So when Windows-targeted malware invades, all of a machine's software functionality is disabled.

A Hypervisor is software that virtualises computer hardware to create Virtual Machines (VMs). Installing Windows on a VM works the same as installing it on actual hardware.

Conversion of installed Windows systems to VMs is straightforward using the free program Disk2VHD which can be downloaded from Microsoft.

On typical modern computers a Hypervisor can easily run multiple VMs simultaneously.

When malware invades Windows that's running on a VM, only that VM is affected.

To speed up recovery you can set up replacement Windows VMs ahead of time, and then copy each to the relevant machine later. Preferably prepare them on isolated VM Maintenance Machines so that malware can't get to them.

So just changing to using VMs can reduce downtime. But with Windows VMs you have to wait until the Windows malware is definitely gone before trying to resume operations.

Note that if you use MS's Hyper-V, which is usable only on Windows-based machines, it's possible that Windows malware will affect it. Requiring a reinstall of all the software that runs directly on the machine, further delaying resumption of operations.

So we recommend instead enjoying the benefits of using an Enterprise Linux based Hypervisor, which is naturally immune to Windows malware. Its component parts are free to download and use, and which you can install and customise. As an alternative we offer a service that creates customised versions and installs them remotely.

Further information : https://iopen.co.nz/docs/virtual_machines.pdf

Desktop Fallback

With a VM-based system, on desktop machines make available an additional VM that runs an Alternative Desktop system which is immune to Windows malware and which can also keep operational data flowing.

So when Windows malware invades your desktop Windows VM you can switch to the Alternative Desktop VM and continue working, even with the malware still around.

If a desktop machine has enough memory (RAM) you can run both VMs simultaneously. Which enables work to be done routinely on the Alternative Desktop, and reduces the amount of work-switching that has to be done when Windows malware invades.

We recommend a Linux-based Alternative Desktop. You can download and install and customise such desktops. Our service includes supplying a customised Fedora Linux MATE desktop VM.

Further information : https://iopen.co.nz/docs/desktop-fallback.pdf

Malware Defeating File Sharer

A Windows-compatible file sharer. Supplied as a VM.

MDFS complements Desktop Fallback by remaining operational and thus able to provide Alternative Desktops with operational data.

Malware on Windows desktops can attack files in shares that the desktops are connected to, so MDFS runs software developed by us that defeats such attacks.

MDFS is based on an Enterprise Linux (EL) and so is naturally immune to Windows malware. It's also protected from other malware by security sub-system SELinux that, amongst its many capabilities, defeats unknown threats.

Further information : https://iopen.co.nz/docs/mdfs-client-experience.pdf
https://iopen.co.nz/docs/mdfs-structure.pdf
https://iopen.co.nz/ws_mdfs.html

Data Backups with Maximum Safety and Availability

Although MDFS effectively defends your data, there's always the possibility of hardware failure, so frequent automatic backups are vital.

In making backups we use the safer 'pull' method.

See : https://iopen.co.nz/docs/backup_overview.pdf

We think it's vital for businesses to retain control of their operational data, meaning keeping it, and backups of it, on hardware that they own.

Thus we recommend in-house backing-up to at least 2 devices located in the homes of managers or executives or in other offices of the business. Those devices automatically pull data from office servers via a dedicated VPN.

We also offer a service that does secure backing-up to our backup servers in case a business wants extra assurance. It can be used in addition to the in-house variant.

See : https://iopen.co.nz/docs/backup_options.pdf

For VM-based systems there's a backup option called a warm-spare VM, and we've documented how to create and maintain them.

See : https://iopen.co.nz/docs/vm-warm-spare.pdf

Keep your data close and your backups safely-close.

Our Motivation For Producing This

We want businesses to achieve better outcomes, regardless of whether we're directly involved in making them happen. Such outcomes can produce effects that benefit many, including ourselves.