Productivity Enhancement and Protection
Improving Business IT Resilience
Graduated Benefits

2024-05-18

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

It's clear to us that you're all doing the best possible with the defensive technologies available to you. But evidently those technologies are not effective enough.

We're also acutely aware that by the time you detect signs of a malware invasion it's almost certainly too late to prevent major operational flow disruption and big costs. A reliable source has stated that only around 10% of invasions get publicly reported, which is consistent with what we've been hearing.

Fortunately, recent advances in technology have made it feasible for us to create an extremely effective defence of what really matters to businesses. And which gives adoptees competitive advantage in at least two ways - protection and profit.

It involves a more resilient way of operating your current IT system. So it's not something that can fit the business model of conventional suppliers, since they prefer to sell you box products and subscriptions.

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

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

The full effects of sudden flow disruption (blood or data) are 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 IT in that we expect malware to invade a business's IT system.

But that the business continues to operate regardless, due to the benefits of the technology and techniques we provide that keep operational data flowing.

The approach is a carry-over from aviation, where pilots train to handle engine failures and other emergencies regardless of the likelihood of encountering them. Because being unprepared for them frequently results in people suffering major injury or death.

Similarly, businesses need to prepare to handle malware invasions regardless. Because being unprepared frequently results in businesses suffering major financial injury or death.

How would you feel if you were on a flight and the captain came on the intercom and said that the pilots hoped they wouldn't encounter any unusual events because the aircraft had

only basic safety systems? Now imagine the business IT system equivalent.

Our resilience scheme gives you control. You decide how much benefit to get, and how much downtime there'll be when malware invades. It gives you competitive advantage via publicising your exceptional commitment to protecting client data and shareholder value.

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

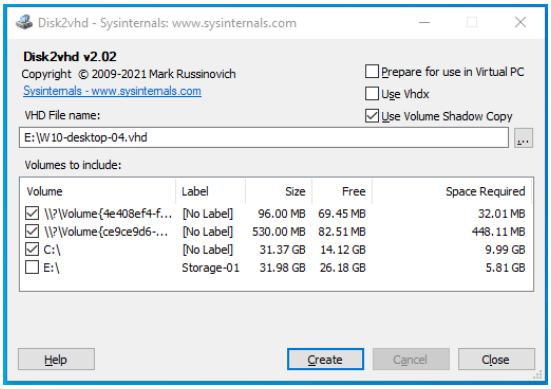
There's currently 3 categories of client for our Business IT Resilience Improvement components. Enquire for details : https://iopen.co.nz/ws_contact.html

The following are the major components of our approach. The technical aspects of the descriptions are intended for your IT support people :

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, as does using it. Typical modern machines can run multiple VMs simultaneously.



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

It's much easier to manage Windows that's running on a VM rather than on the actual hardware.

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

To speed up recovery from invasion you can set up replacement Windows VMs ahead of time and under low pressure. Then copy each to the relevant machine at the appropriate time 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.

Also 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 too. Meaning that for safety all the software that runs directly on the machine should be reinstalled, further delaying resumption of operations.

Instead you can enjoy the benefits of using an Enterprise Linux based Hypervisor, which is naturally immune to Windows malware. The component parts are free to download and use, and you can install and customise them. 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.

The desktop that we use and recommend is as easy to get to grips with as a new car is.

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, and easily switch between them using keyboard hot-keys.

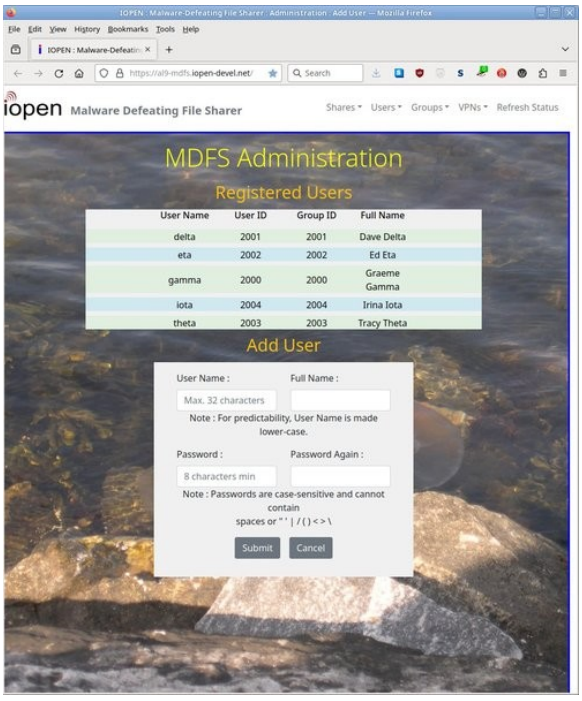
Which enables work to be done routinely on the Alternative Desktop, and reduces the amount of work-switching that has to be done when Windows malware invades.

We recommend Fedora Linux MATE (mah-tay) for the Alternative Desktop, since it comes with the superb SELinux security module enabled. You can download and install and customise it. Again as as alternative, our service offerings include supplying customised VMs that run it.

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 it 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.

It also enables having file shares that only Alternative Desktops can access. Perhaps store critical or ultra-sensitive data in such shares, so Windows malware can't access or affect it in any way.

Gradually evolve your use of the scheme under low pressure so when an invasion happens your staff can make a smooth and rapid transition to full-Fallback.

Furthermore, if on your network you organise machine addresses appropriately, then it's straightforward for us to make the MDFS firewall able to deny access from Windows machines whilst allowing access from Alternative Desktop machines. So that during a Windows malware outbreak it's possible to prevent the malware interfering in any way with the continuing operations.

Further information : https://iopen.co.nz/docs/mdfs-client-experience.pdf
https://iopen.co.nz/docs/mdfs-structure.pdf
https://iopen.co.nz/ws_opdataflow.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 MDFS and other 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

Note that our MDFS has a dedicated backup channel (a dedicated VPN), which improves security and also avoids legitimate backup runs degrading checking for signs of malware doing file exfiltration.

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 operating data close and your backups of it safely-close.

Linux

You and your IT support people need not be concerned about the introduction of Linux into your business. It's simpler and can be used much more securely than Windows, and even Microsoft are promoting its use.

It also runs many devices, including ones in motor vehicles, and very likely you have devices that use it.

Your IT support people will benefit from learning how Linux can boost system security. Especially via security module SELinux, with its ability to defeat unknown threats when operating in Enforcing mode.

We use and provide Enterprise Linux variants AlmaLinux or Rocky Linux for all server-like situations because by default they have SELinux:Enforcing. For desktops it's either Fedora Linux MATE or Rocky Linux MATE. Fedora Linux also has SELinux:Enforcing.

MS-Windows doesn't have anything even close to SELinux's capabilities, and it shows.

Basis Of Our Charges

Almost all of the software involved in this scheme has a Free Software licence. Free as in freedom to copy and install and use. As with all IT systems there is a need to select the appropriate software packages and configure them appropriately after installation.

Thus the basis of our charging is similar to that of lawyers and accountants. In principle your business can do all its legal and accounting work itself, but you outsource the work to them in order to benefit from expertise and reduce the risk of mistakes, and pay the resulting significant fees.

If you use this operational-flow-maintaining scheme at close to maximum benefit you can expect very rapid payback after a Windows malware outbreak starts.

At an appropriate point we will commence donating a percentage of our profits to relevant Free Software projects.

If you decide to do some of the work yourselves it's vital to download Free Software packages from official servers. Some packages downloadable from non-official servers have been modified in unacceptable ways.

Software that we develop which has security implications is licenced to individual clients, and we provide them with a copy directly. To prevent the distribution of corrupted or backdoored copies.

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.