Infrascale™

A TALE OF TWO RANSOMWARE VICTIMS

"With Infrascale Disaster Recovery we were able to restore our client's data and operations within one hour."

Jason Miglioratti, *Director of Managed Services*

PERVASIVE SOLUTIONS

PROFILE

Pervasive Solutions is a managed service provider (MSP) and information security consulting firm that provides its customers with the solutions they need to reduce costs and mitigate business risks.

PARTNER CHALLENGES

- Help clients take a proactive stance to disaster recovery, protecting them from micro- and macro disasters
- Protect all of their clients against ransomware attacks and other threats to downtime and financial loss
- Educate their clients' end users about the threat of ransomware and best practice guidance for recognizing phishing attacks

SOLUTION

Pervasive Solutions has started evangelizing the benefits that a DRaaS solution has to offer to their clients and has deployed Infrascale Disaster Recovery across a number of customers to address ransomware and other threats causing downtime and resulting in financial loss.

BACKGROUND

Just after Thanksgiving last year, Jason Miglioratti, Director of Managed Services at Pervasive Solutions, discovered that two of their clients had been infected with ransomware within the same week. Jason's experiences with these two clients were vastly different because of the underlying infrastructure and safeguards that were in place. In this case study, we will compare and contrast Jason's experiences with each client to demonstrate the importance of security training, anti-virus, disaster recovery as a service, and regular DR testing.

	RETAILER	MANUFACTURER
Amount of Protected Data	35-40 TBs	10-15 TBs
Locations	40-50	3
Strain of Ransomware	Locky	Locky
When Infected	November 2016	November 2016
Data Infected	File shares, ERP (Great Plains)	File shares, ERP (MAS90)
Server Protection	Microsoft Data Protection Manager	Infrascale Disaster Recovery
Restored Operations	2-3 days	< 1 hour
Fully Restored	2 weeks	< 1 hour
Man hours spent	320	< 1 hour

RESULTS

- Defined process for mitigating ransomware infections with validation
- Recovery of all data (zero contamination)
- Client's production environment restored in less than one hour
- Ability to provide a more holistic security solution to combat ransomware

"It's no longer good enough to get your clients' data back in a few days -- now you need to restore operations in minutes."

Jason Miglioratti,
Director of Managed Services

ABOUT PERVASIVE SOLUTIONS

Based in Victor, New York, Pervasive Solutions is a managed service provider serving a variety of industries across the Northeast. Pervasive separates themselves from typical IT providers with a specialty in security services in addition to traditional IT services and support. The mission of Pervasive Solutions mirrors that of Infrascale -- to protect the data, uptime, and operations of its customers. This is reflected in the services they offer – everything from security risk assessments, regulatory pre-audits, penetration testing, and even social engineering testing – all intended to posture their clients' security systems as a strength, not a weakness.

Pervasive Solutions has been an Infrascale partner since May 2016 and currently recommends Infrascale Cloud Backup and Disaster Recovery solutions as part of their security and data protection services.

CUSTOMER A: RETAILER

On the morning of November 30, 2016, Jason was notified from the IT administrator at a local retailer that they thought they had been infected by ransomware. The administrator noticed that most of the files within a file share had been encrypted and were inaccessible. At this point, Jason and his team of three engineers sprang into action. The first order of business for Pervasive was to determine how many PCs were infected and to start scanning all of the PCs and servers in the network. Without the standard toolset in place (including Infrascale and Sophos), it was difficult for them to identify the point of entry of the malware. Making matters worse, the retailer's onsite backup was also infected with the malware preventing a recovery of the DB.

Because the retailer doesn't have a DRaaS solution in place, Jason did not have the ability to quickly spin up clean VMs or perform restore operations. Instead, Jason and his team had to restore clean files from a secondary SAN, one file at a time. This allowed Jason to get the retailer "semi operational" within 2-3 days. This meant that the email and their ERP (Microsoft Great Plains) systems were up and running within 48 hours, but non-mission critical apps and file shares were not fully restored for another two weeks. For Pervasive, this was an all hands on deck exercise which meant that Jason and his team worked around the clock to restore clean copies of their files and get their customer fully operational.

CUSTOMER B: MANUFACTURER

A day after the retailer was infected, Jason received an anxious call from a finance clerk at a local manufacturer, another client of Pervasive, concerned that she did something that she desperately wanted to undo. The clerk went into her spam quarantine and clicked on an email attachment mistakenly assuming it was an invoice that needed to be paid. Once clicked, the malware -- a variant of Locky – went cruising through and infected a large swath of files on their network (i.e., almost 500,000 files were encrypted in less than six minutes). Jason was able to pinpoint the machine that had been infected with the help of an endpoint protection solution deployed by Pervasive. Just as with the retailer, Jason started scanning all of the PCs and servers on the network to determine the extent of the infection and began the painful process of recovering clean versions of the infected files. It was at this point that Jason appreciated the power and value of the Infrascale DRaaS solution which had been installed a month before. This meant that he could actually spin up VMs of the backups from the local, on premise appliance, instead of manually restoring files – one at a time.

RESULTS

- Defined process for mitigating ransomware infections with validation
- Recovery of all data (zero contamination)
- Client's production environment restored in less than one hour
- Ability to provide a more holistic security solution to combat ransomware

> It is no longer good enough to get your clients' data back in hours, they want their operations back in minutes. With Infrascale Disaster Recovery, we can actually do this."

Jason Miglioratti,
Director of Managed Services

Jason booted up several recently backed up VMs, one after the other. He knew that an infected VM would not properly boot. Jason then proceeded to quickly restore the infected file servers, email and ERP (MAS90) applications – all within 5 minutes – and without the help of any additional technical personnel at Pervasive. The contrast between the retailer and manufacturer is dramatic in terms of the disruption, downtime, and effort caused by the ransomware events. This is why Jason now recommends Infrascale Disaster Recovery to all of Pervasive's customers.

KEY TAKEAWAYS

As Jason reflected on both events, there are a number of insights gained from the experience – some obvious, some more subtle. These include the need for Pervasive to:

- Have a DRaaS solution in place that can reduce the ransomware mitigation process from hours (or days) to minutes.
- Quickly identify the point of infection. DRaaS can be leveraged to identify the infection date: if a VM does not boot properly, it has probably been infected by ransomware. In this way, the administrator can then restore from the next most recent VM.
- Educate all of its clients about the importance of DRaaS in mitigating the damage of a ransomware attack and the real impact it can have on their business.
- Regularly test their clients' DR plans so they have the confidence to know they can recover from any disaster.
- Encourage all of their clients to deploy commercial-grade protection to quickly identify and isolate entry point of infection and determine the extent of the infection.
- Modify their escalation process in the event of an incident. With Infrascale, VMs can be booted within 15 minutes, so Pervasive must be able to reconfigure their network so end users can quickly access their applications.
- Incorporate DRaaS and DR testing as part of their regularly scheduled security audits.

THE AFTERMATH

Computer viruses and exploits are occurring at an ever-increasing rate. Hackers now operate at highly professional levels and are very good at what they do. In fact, they even outsource their skills and attack schemes so other people can participate successfully without having the skills themselves. Without having a data protection and recovery strategy in place, organizations are leaving themselves wide open to significant financial and reputational loss.

Pervasive Solutions is part of a new and emerging group of MSPs that are going well beyond reselling solutions or providing networking services. They're educating their clients that data protection requires a four-pronged approach which includes user education, strong security systems (e.g., AV, firewall, email-filtering, application white-listing, etc.), cloud-based disaster recovery, and regular DR testing.

Pervasive's recent experience with ransomware is helping them evolve their security practice and the guidance they dispense to their clients and prospective clients. By making DRaaS the focal point of their practice, they can better protect their customers against ransomware, regulatory penalties, and costly downtime while making their services far more "sticky" and indispensable. This is enabling Pervasive to more of a strategic partner to their clients than just a mere cost center.