DASHBLACK WHITEPAPER

Ransomware – A Possible Solution

June 2018

Ransomware has been devastating the world from a digital perspective since roughly 2012 (according to Wikipedia https://en.wikipedia.org/wiki/Ransomware) and has been a growing epidemic.

At Dashblack, we have had a few cases of ransomware-infected clients but were lucky enough to have a decent backup solution in place from which we could restore all the client's data.

There are some tech companies who claim they can decrypt your data for a hefty fee, and again, this is not foolproof. Furthermore, a study done in **2014** suggests that it could take up to 5 Quadrillion Years to decrypt your data (RSA at 256 bits) with the technology at the time.

So, where does this leave us? Is prevention better than cure?

Assuming you have a good backup solution: you could *to some extent* relax since your data is backed up to one of our, or another, cloud backup provider so your data is safe, but what you should be thinking about are these two terms:

RTO and RPO. They stand for Recovery Time Objective and Recovery Point Objective.

What this means is: RTO talks to how quickly you can get your data back once a disaster such as Ransomware has struck, whereas RPO talks to when last your data was backed up.

Now, let's play a numbers game. Here is the scenario:

- You have 50 staff in your company and a critical server is hit
- Your last successful backup was 24 hours ago
- It will take your backup 2 days to download from the cloud (Given RSA bandwidth)
- Now, it will take the technician 8 hours to reload your server and restore your data

This equates to 80 hours of downtime.
Working on a margin of an 8-hour work-day we can divide that number by 3, which gives us 27 hours.

27 (work) hours times 50 employees equate to 1350 man-hours lost (and this was a conservative calculation based upon real-world recovery strategies).

How much are your employees' worth per hour and what potential client-service loss will your company face during this time?

The long and the short: Ransomware sucks and can bring a company to its knees.

So, what do you do?

- Having a good antivirus is an excellent starting point
- Ensure your mail provider has a decent spam filter
- Ensure your firewalls are updated and managed, not just installed and left to the wolves
- Have strong Wi-Fi passwords, and maybe even MAC address filtering to only allow certain devices to connect
- And the single most important thing you can do to protect yourselves? ***USER EDUCATION!***

From our personal experience, nine out of ten cases of Ransomware were due to an end user clicking somewhere they shouldn't have. This is typically a file received via mail and could even have been received from a known and trusted sender.

The sender, however, may not have sent it, but his address could have been spoofed, meaning that someone else (with malicious intent) used his email address to send on his/her behalf.

And, you are infected!

Q

So… How do you protect all your staff from all the world's malicious senders?

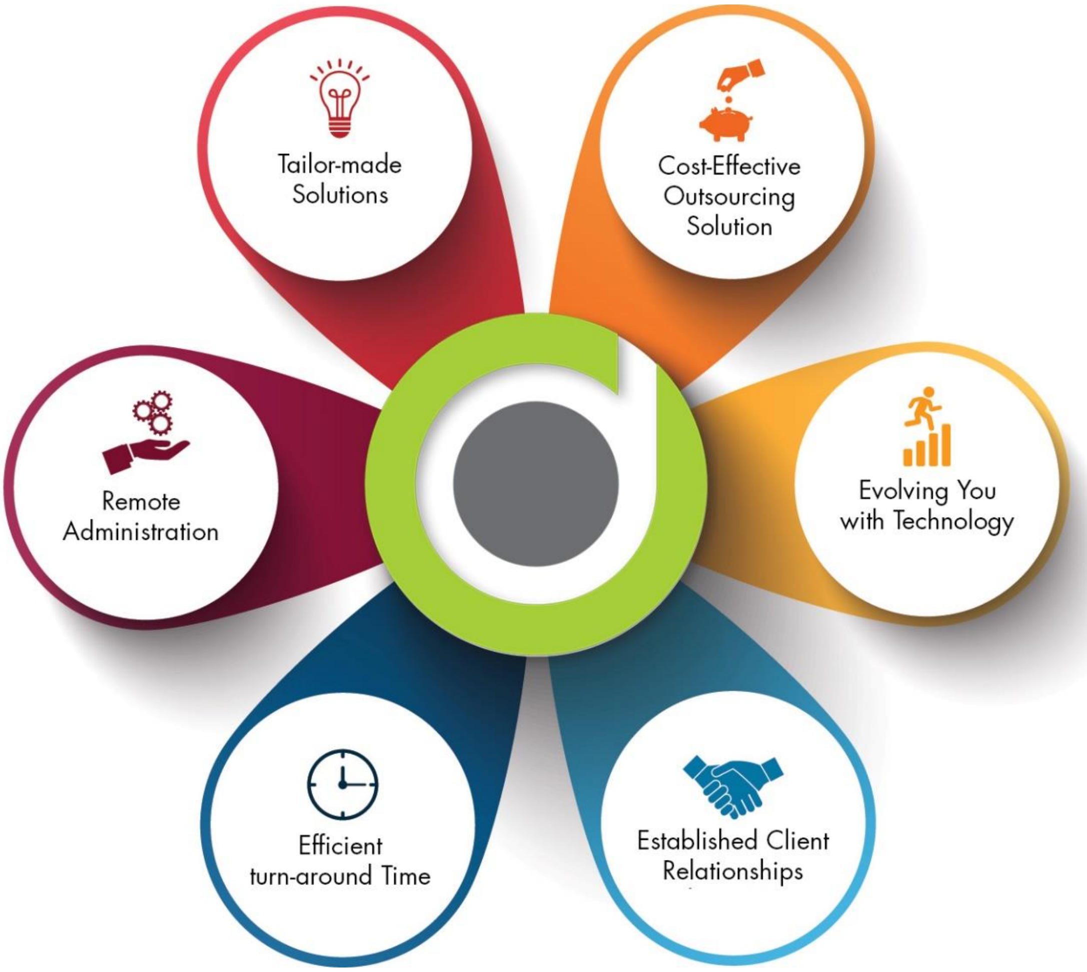
A

We have set up a mail address which we encourage your staff to use. Forward any suspicious emails to us and we will revert informing if it is valid, or malicious.

We are a group of engineers that have a tad more technical knowledge than the average end-users and offer this help free of charge to the public.

Send any suspicious emails to care@dashblack.co.za and we will check it out for you for free.

We hope this free service reduces the risk of infection across SA. Now all that is needed is for you to use it.


Tailor-made Solutions
Cost-Effective Outsourcing Solution
Remote Administration
Evolving You with Technology
Efficient turn-around Time
Established Client Relationships