Building strong and effective defences against ransomware.

03 June 2020

Earlier in the year, I wrote a blog describing how organisations could build a secure last line of defence against ransomware. Since that article was published, of course, the world has become a very different place and my first thoughts are with everyone having to deal with this crisis both professionally and personally.

Different world, same threat

Unfortunately, what hasn’t changed is the pervasive threat of cyberattack. Recently, the FBI warned that cybercriminals were taking advantage of the Covid-19 crisis to exploit the growing use of virtual environments. With so many workers forced to login remotely from improvised home offices, criminals have many more openings they can target to gain unauthorised network access.

Meanwhile, hackers are taking advantage of public concerns by using phishing emails, disguised as official bulletins, to try and spread their malware. Cybersecurity provider, Cybereason, has reported numerous examples of coronavirus-themed emails whose purpose is to persuade individuals to open messages that under normal circumstances, they would ignore.
Building strong and effective defences against ransomware.

Example of a coronavirus-phishing email (Source: Cybereason)

Five simple steps to tackle ransomware

So what can you do as a company or individual to guard against the threat of cyberattack? Here is a simple five point plan that will go a long way to helping you secure your defences.

1. Make sure that (as far as possible) your servers and PCs are up-to-date with the latest operating systems and antivirus solutions.
2. If not, consider if older machines, (which you might not be able to update or support any more), could be replaced or retired. The cost and inconvenience will probably be less than the impact of a cybersecurity breach.
3. The third straightforward step is education: making sure everyone in the organisation, not just in IT, is familiar with ransomware methods and can recognise phishing attempts to gain password credentials or circulate harmful links and attachments. Larger companies employ so many different and diverse professionals, covering a multitude of functions, that there needs to be a culture of vigilance across the entire organisation. For that reason, a dedicated IT Security Executive can be seen as an essential leadership role to help co-ordinate both preventative planning and an effective response when ransomware does strike. If present circumstances make this a challenge, subscribe to cybersecurity bulletins that will keep you up-to-date with known current threats and use these to inform your colleagues.
4. For more specialised IT teams, it’s also important to use different credentials for accessing backup storage and maybe even a mixture of file systems to isolate different parts of your infrastructure to slow the spread of ransomware. In the event of a ransomware attack, criminals will go after your backups as well and if a recovery file is corrupted with ransomware, it could also be inaccessible. One way to stop this is to use an array like HPE StoreOnce that isolates your backup from traditional lines of communication and command sets leveraged by ransomware attackers. Avoid using obvious credentials, like Domain/Admin to gain access to your backup volumes. And if you outsource to an MSP or CSP, audit their ransomware defence protocols. Do they use encryption? What are their SLA’s for business continuity and restoring data? It’s definitely worth running fire drills for the worst case scenario so that you can have a set of processes to fall back to when ransomware strikes.
5. And finally, follow the 3-2-1-1 rule. Three copies of your data, on at least two different media, with one stored offsite (e.g. cloud or tape) and one stored offline (e.g. tape). During a cyberattack, HPE StoreEver tape can provide a vital last line of defence because you can maintain copies of your data fully offline behind a physical air gap. Cyber criminals may access your production and storage domains using stolen credentials but they cannot compromise data that is kept on AES-256 encrypted cartridges in a secure vault. The ultra low cost per GB and rapid transportability of HPE StoreEver tape media complements your flash, disk and cloud storage. Tape can’t help you recover instantly, but it can greatly speed up your recovery in the hours and days that follow.

We had data replication set up to an offsite disaster recovery site, forgoing traditional tape backups. Guess what? The cybercriminals targeted that data as well. Tape backups and an air-gapped solution are an absolute necessity.

Jeremy Bayness, CTO, Bag Makers

Although these are challenging times now, more than ever, it’s important to maintain your defences against the threat of cyberattack so that your business can remain safe and connected. HPE StoreEver tape solutions is here to help you meet your most immediate challenges and unexpected demands.
3. [https://www.reddit.com/r/sysadmin/comments/63gs2s/update_to_got_hit_bad_tonight/](https://www.reddit.com/r/sysadmin/comments/63gs2s/update_to_got_hit_bad_tonight/)

Andrew Dodd  Andrew Dodd

Worldwide Marketing Communications Manager at HPE Storage

Other posts by Andrew Dodd

Contact author Twitter