WHY BUSINESSES NEED TO UPDATE THEIR DR PLAN NOW

With cyberattacks becoming more common, and natural and man-made disasters not going away, disaster recovery programs are more important than ever.

August 1st, 2017 • Information Week • Kevin Beasley

The first half of 2017 has seen some of the biggest cybersecurity attacks to hit companies around the world. In May, WannaCry ransomware ripped through hundreds of thousands of computers worldwide, encrypting files and demanding payment. This attack was closely followed by NotPetya in June, which infected tens of thousands of computers in 65 countries. Although these large-scale attacks make global news headlines, the reality is that attacks like these happen every day with businesses of all sizes being vulnerable targets.

No company is immune to a cyberattack, so having a disaster recover (DR) strategy is crucial to minimizing data and financial loss. However, if you create a plan and then neglect to test, adapt, and review it, you risk overlooking defects that can leave your assets unprotected and the consequences can ultimately shut down your business.

Malware is a constant threat, and cyber criminals are always developing new ways to infiltrate the most protected systems. As businesses add more systems and applications to their networks, those who don't regularly update their DR plan run a higher risk of becoming victim to a devastating malware attack.

Traditionally, many businesses have used static DR plans, establishing a fixed configuration that is reviewed on a yearly basis at most. With cyber-attacks becoming more sophisticated and persistent, it's time businesses update their DR plan dynamically to reflect current best practices.

Businesses are using more applications, and systems are becoming more complex, allowing infrastructure to quickly outgrow a static plan. Anytime a business adds or re-deploys an application, the DR plan should be re-evaluated to ensure the updated infrastructure and applications are fully covered.

Although cybersecurity is one of the biggest threats facing businesses, localized disasters such as fires, broken water pipes, and natural disasters can cause significant outages and costs that you can only prepare for if you have a DR plan. This is why one of the most important and basic components of DR planning is keeping up-to-date, complete inventory of all devices and applications, as well as the vendor technical support information.

Similarly, all DR plans should take note of personnel involved with the DR plan, with clearly defined key roles and responsibilities with

InformationWeek

Vormittag Associates, Inc.
A Leader in Enterprise Management Software
www.vai.net

cross training. If disaster strikes, the last thing you will have time for is to explain to staff what the plan is and what their role is. Keeping staff updated on the DR plan by the DR planning team helps to cut down on chaos and enables you to respond to the crisis more efficiently and in a timely manner.

It is important for all DR plans to establish a recovery point objective (RPO) and a recovery time objective (RTO) for each application. This will define each device and application's tolerance for downtime and data loss. By setting realistic RPO and RTOs, businesses can prioritize what applications or devices need to be addressed first when hit by disaster in order to have the most efficient response. As new devices and applications are added to the network, RPO and RTOs should always be evaluated to ensure priorities are in order.

One of the most vital parts of an effective DR plan is a guide on how sensitive information will be protected, maintained and accessed when disaster strikes. In an era where we have more data to store than ever, and given that most malware includes taking or disrupting sensitive data, this component of a DR plan should always be evaluated and updated with the latest best practices.

Finally, DR plans can be great in theory, but if it they are not put to test, you never truly know its effectiveness. Hiccups in DR can be as complicated as backup applications failing or as simple as a DR employee being out of the office that day, but in the end, those challenges will weaken a DR program. Testing the plan more than once a year ensures that all wheels are moving smoothly.

With large-scale cyberattacks becoming more common, and taking into account the thousands of smaller attacks that occur on a daily basis, DR programs are more important than ever. Continually evaluating and updating a DR plan and testing it on a regular basis is the difference between a business ruined and one that can easily bounce-back. Cyber criminals and their malware may be always finding new ways to get into systems, but by continually planning, businesses can stay one step ahead.

InformationWeek

Vormittag Associates, Inc.
A Leader in Enterprise Management Software
www.vai.net