TREXIN INSIGHT PAPER

October 31, 2018

FINDING YOUR GAPS

Knowing your weaknesses in an ever-changing landscape.

If you are part of the IT world then you likely know your company's Business Continuity/Disaster Recovery (BC/DR) plans inside and out. In addition, you likely played a primary role in building them. On paper everything probably looks great, but when was the last time you tested it? When was the last time you pulled the plug on a server to make sure your uninterruptible power supply (UPS) kicked in or made sure your generators worked as intended? What is your backup plan if Exchange goes down?

In most IT environments, testing for outages is straightforward and if something fails to do what it is supposed to do, you are generally nearby and able to fix the issue. However, not everyone works in a standard IT environment these days, so testing for outages isn't necessarily as straightforward as it used to be. For a moment, picture yourself as the IT Director for a company that is 100% cloud-based. How do you test for outages and mitigate them if they did happen? In this scenario, if your UPS fails to kick over you cannot just run down to your data center and fix it, you cannot just fire up a backup mail server to fix your issues either. Finding your gaps is one of the most important things when it comes to BC/DR planning because nothing in this world ever goes as expected.

I am the IT Director at Trexin Consulting, and we fall into the "unique" category when it comes to our IT environment/infrastructure. We are a virtual company, which means we don't have our machines on a network. More importantly, I do not have a data center I can run down to when things go sideways. We must rely on the cloud for 100% of what we do. Coming from a traditional IT structure to one like we have at Trexin was like trying to climb a mountain without any climbing gear. Everything I knew from my past experiences no longer applied here, as I could no longer physically touch any of our equipment. This makes planning for and testing BC/DR plans that much more challenging. This also means that unlike a standard BC/DR plan, you cannot actually test it because there is no way for you to just shut down your mail server to see if your failover works. So how do you know if your BC/DR plan works? How do you find your gaps?

As most of you probably know, Microsoft had an outage on Tuesday, September 4th, that severely impacted various Azure services; you can read the postmortem here if you haven't already. Like many companies these days, we rely on Microsoft's Outlook 365 offering to provide most of our infrastructure, however, unlike most companies our size we don't have an on-site Active Directory (AD) to manage since we are a virtual company. Luckily, during this outage AzureAD wasn't affected. We must rely on Microsoft to have a robust DR and failover in place in the event that they have an outage. Luckily, we had gone through our annual BC/DR simulation prior to this outage. Based on the title of this article, you can assume that once we started to move down the BC/DR path we found gaps that we had not accounted for. We leveraged a continuity service from another company that allows us to failover email if O365 goes down. This is just an example of one of the handful of gaps we were able to uncover as we moved into our BC/DR plan.

When an outage happens it's important to keep your head on a swivel, so that you may be better prepared if something isn't going as planned. In our case we were able to quickly move away from the Security Assertion Markup Language (SAML) integration and into another authentication method so our users could leverage our email failover platform (if needed). BC/DR plans are only as good as the paper they are written on if you actually test them and for those of us who can't actually test them, then we have to use our years of experience and a little luck to navigate through the minefield that is a continuity event and hope we come out the other side unscathed.

AT THE END OF THE DAY

Our problem is one that likely affects many companies. We rely too heavily on one authentication method, and if that authentication method becomes unavailable then we would have no way for our users to do what they need to do. The importance of having a backup authentication method is paramount in maintaining continuity during an outage. For companies like Trexin, having a backup authentication method is harder to come by, but for everyone in a traditional company, this is something you need to account for during your annual BC/DR planning meetings/tests. Whether you have a backup AD onsite that you can failover to or you use some sort of third party directory solution, the less the users see of the outage the better it is for your poor Service Desk person.

This TIP was written by Mike Herman, Trexin's IT Director. Mike welcomes comments and discussion on this topic and can be reached at mike.herman@trexin.com.