Marshall Eddy

CS331-001

Vincent Skimmer

26 September 2016

Recovery from Ransomware

When dealing with a cyber security breach clearly the best way to recover from this is by having a backup. However, you may not know that there even is a breach in the first place, as the attacker could be quiet. So, first you need to identify the problem and form a task force, isolate the damage, begin the remediation process, and develop a communication strategy.

Identifying the problem is one of the most important first steps in the recovery process, and timing is crucial. Once the issue is brought to your attention you must quickly gather the crisis communications team and begin answering questions that will provide insight into the scope of the attack. The task force makeup varies but it should consist of senior executives, public relations professionals and legal counsel (kcdpr). A representative with an IT background will be helpful for this process as well. You’ll want to be answer the following questions to be able to take the correct next step: When was the breach noticed? Which services, systems, etc. have been affected? What type of attack is it? Who committed the attack and do they have an agenda? Who or what is the target of the attack?

Some ways of noticing a data breach can be if your computers are slower than normal, or lagging, if there are pop-up windows that you can not close, increase in spam emails, or unusual websites asking for your business credentials. Once you’ve figured out something is wrong, you need to check and make sure if any data was altered or encrypted before moving on.

Data breaches should be approached in the same way firefighters handle a fire (kcdpr). The affected areas need to be isolated to prevent spreading and to protect against additional vulnerabilities. Quarantine the corrupted servers, devices and systems so they can be examined and made functional again. Most cases, recovering compromised data is impossible, so it would be unwise to give in to any demands, if it is ransomeware. Your best bet is to always make sure you have a backup and continuously update it so no new data is lost. If you have noticed data has been effected on one computer, it would be wise not to use any computers that can be connected to the server until the problem is resolved.

Now that the breach has been dealt with, you’ll need to start the recovery process with information security professionals to asses the damage and begin cleaning. Work with the crisis communications team and IT representatives to evaluate the extent of the damage and keep a record of the findings. This will provide a baseline from which to measure the effectiveness of the remediation efforts once they have been completed. Next, the teams will need to establish a hierarchy of need by focusing on the more critical areas initially and then moving onto less essential areas until completing the process.

The crisis communications team must identify each of the audiences that need to receive information about the data breach. Typically, audiences are separated into internal and external groups. The internal group generally consists of employees, business partners and stakeholders while the external group can include clients and the general public. Decisions about the manner in which the messages are delivered and the timing for each also need to be made.

In the end, data breaches and ransomeware are a real threat that everyone and every business is open to attack, no matter how strong your defense is, they can still find their way in. The best thing to do is have a backup and try and keep sensitive information offline or only accessible through one or two reliable and intelligent employees. If it is ransomeware you are have to deal with, then having a backup is your only recovery method. Hopefully you will be able to wipe your hard drive and re-install all the information to get your computer up and running again, but worst comes to worst, you would have to get a new hard drive, which is not too costly if it is just a personal computer. But when it comes to a business, if every computer connected to the server needed a new hard drive, then the price will be quite high. For this reason, you will want to be able to detect the breach as soon as possible and put an end to it before it is too late.

References

Textbook for CS331

<http://www.businessnewsdaily.com/8001-have-you-been-hacked-how-to-recover-from-a-data-breach.html>

<http://www.kcdpr.com/hacked-steps-recovery-cybersecurity-breach/>