CLEAR InfoSec
An Ana-Data Company

Hurricane Florence – Cyber Security Best Practices

"Unfortunately, when disaster strikes cyber criminals are always right behind, ready to apply social engineering techniques to take advantage of both the victims and people wishing to help."

While Hurricane Florence ravaged the south eastern part of United States mostly Carolina's with strong winds and heavy rains. During this time, the cyber criminals are busy figuring out how they can capitalize during this catastrophic event. It is important that we implement the necessary safeguards, and ensure they are effective in restricting the cyber criminals from getting unauthorized access to company's infrastructure and leveraging sensitive information.

Cyber criminals always take advantage of natural disasters such as hurricanes, to compromise sensitive data and infrastructure. They will easily leverage this turbulence period, to conduct social engineering, phishing or even try to get physical access to the company's data center. A recent survey conducted by IBM indicated that the average cost of a data breach is $3.62 million, and these figures are expected to get exponential during disasters. This is something no organization wants to deal with. Every company must be able to withstand not one, but multiple cyberattacks as we are dealing with CYBER CRIMINALS, who are known for their disdain.

From our experience, the cyber criminals usually target the financial data, as financial gain is the biggest motive of most of the cyberattacks. The cyber criminals do not empathize the situation and attack the organizations leaving victims helpless. The victims could find that their bank accounts have been manipulated or even worst all the money disappearing from their bank accounts. It is strongly recommended that every organization should not only back up all the critical data but also ensure that they are encrypted. Critical financial and personal data can fetch billions if sold on dark web.

Phishing

Typically, cyber criminals send phishing emails to the employees and customers to get the initial foothold leading to complete compromise of the IT infrastructure. Cyber criminals try impersonating as IT technician/support team and trick employees or even customers to give out sensitive information like system passwords, account information, financial information etc. Cyber criminals utilize the heat of the hour, when disaster strikes, and send phishing emails with current updates on natural disaster, which most of us are bound to know more, and this percentage of anxiousness will increase if we have our friends and family included in the list of affected people. Cyber criminals even try sending links which redirects them to a website where they can send in their donations to help the people affected by the hurricane. We click on the link thinking our donations would be of some help to people affected during disasters but end up depositing funds into the cyber criminal's account following the deceptive link.

Best Practices to Follow

It is very important that we educate all the parties, including customers, employees, suppliers, stakeholders and vendors about the awareness on phishing/social engineering on a regular basis so that they can stay ahead of the breaches even during the time of natural disasters. From the technology perspective, the minimum baseline is to implement filters at your email gateway to filter out emails with known phishing attempt indicators and to block suspicious IPs at your firewall. Flag emails from external sources with a warning banner, and most importantly "DO NOT TRUST ANY EMAIL."

Many companies feel that all is well, if they have all their data stored on cloud, but even cloud data is vulnerable. It is important that your cloud is protected, monitored, and access management should be the top priority. It is strongly recommended to have patch management and to follow regulatory compliance. Patch management acts as an armour which prevents attacks and protects against various exploits. Along with all the preventive measures, business continuity and disaster recovery should be in place. Cyber criminals often target vulnerabilities and exploit them but should reckon that they also love to exploit natural disasters.

About us

Clear Infosec, an Ana-Data company assists you in providing more insights about how to stay secure. To know more about our information security services please speak to one of our cyber security expert by calling us on 551-236-1031 or email us at infosec@ana-data.com.