AbriteLogic SOLUTIONS

SELECTED CYBERSECURITY CASE STUDIES

Your Partner For A Secure Business

AbriteLogic Solutions
www.abritelogic.com

A RANSOMWARE ATTACK @ COLONIAL PIPELINE

Synopsis of the Attack

In the spring of 2021, news broke in reference to a cyberattack on Colonial Pipeline company–an American oil pipeline system. As a proactive measure and in response to the attack, the company swiftly shut down its pipeline system and halted all pipeline operations to contain the attack. Eventually, the company restarted its entire pipeline system and resumed normal business within days; however, not until it paid millions of dollars as a ransom.

What could possibly be the cause of this attack? Was it due to an insider attached, a leaked password, an inactive VPN account, or a lack of multifactor authentication? It was believed that the hackers breached the company using a compromised password probably retrieved from the dark web. The ransomware cyberattacks crippled the computerized systems and led to a shortage of fuel across the East Coast.

During the attack, the Department of Energy (DOE) and FBI got involved to provide situational awareness, analysis of impacts, support, and other response efforts. This was in an attempt to resume operations without delay while moving fuel supplies to impacted areas to mitigate or minimize impacts to consumers.

What to Expect

Our cybersecurity trusted advisors are available to help provide the necessary visibility across your entire network infrastructure and thus allowing for proactive threat detection and improved incident identification, robust investigation, and rapid resolution.

Additionally, our subject matter experts will help and guide your team to implement cost-saving measures to proactively identify, mitigate, and remediate security threats and potential attacks. In other words, the knowledge gained can be used to inform decisions regarding the enforcement of policy and best practices to stay protected against future attacks to a large extent.

Response, Impact, Root Cause Analysis, **and Lessons Learned**

Want to discuss the response, real impact, root cause analysis, and lessons learned from this attack, and count on us to have the discussion tailored to your needs? Then make a decision now!

The team of cybersecurity experts from AbriteLogic Solutions is available to offer a FREE half-hour consultation to discuss the relevant details along with the security implications it may possibly have on your organization.

THE LESSON LEARNED FROM THE TARGET DATA BREACH

Synopsis of the Attack

Back in the holiday season in December of 2013, the Target retail giant was breached when cybercriminals were able to steal 40 million credit and debit records and 70 million customer records. While this attack wasn't the single largest security breach at the time, it was one of the largest and most impactful in history.

While the target of the attack was the Target retailer, the attackers didn't go directly through Target's network, but rather via a third-party vendor. During the attack, a malicious actor sent a message pretending to be from a trusted person or entity, manipulating the third-party employee and thereby causing a malicious file to be installed. As a result of this action, it enabled the hackers to exfiltrate sensitive information from the company servers. Of course, humans will always remain the weakest link in the cybersecurity chain.

The data breach highlighted one of the major business challenges that occur following the breach. The consequences of this attack were enormous including disruption to business operations, the cost of the settlement to the tune of millions of dollars, the lack of customers' trust, and above all reputation damage. In addition to the settlement, the company was required to adopt proactive measures to secure customer data such as credit card information, hire an independent, qualified third-party, auditor/assessor to conduct a comprehensive security assessment, and other requirements. The victims of this and other high-profile data breaches have suffered horrendous fates.

What to Expect

Our cybersecurity trusted advisors are available to help provide the necessary visibility across your entire network infrastructure and thus allowing for proactive threat detection and improved incident identification, robust investigation, and rapid resolution.

Additionally, our subject matter experts will help and guide your team to implement cost-saving measures to proactively identify, mitigate, and remediate security threats and potential attacks. In other words, the knowledge gained can be used to inform decisions regarding the enforcement of policy and best practices to stay protected against future attacks to a large extent.

Response, Impact, Root Cause Analysis, **and Lessons Learned**

Want to discuss the response, real impact, root cause analysis, and lessons learned from this attack, and count on us to have the discussion tailored to your needs? Then make a decision now!

AN INSIDER ATTACK LED TO A SIGNIFICANT DATA BREACH

Bupa, the global health insurance company, was hit by a massive data breach affecting over credentials of several thousand global customers back in early 2017 after a rogue employee (an insider) inappropriately stole customer information from the company and tried to sell the customer information on the dark web.

Sensitive information extracted in question included such things as name, date of birth, email address, and nationality. The good news was that no medical data, PHI, or financial information was compromised; however, there was no evidence to suggest that the stolen data was used to carry out fraudulent activities elsewhere.

It is surprising to know that even with this insider attack, an anomaly traffic flow due to a large amount of data being extracted would have triggered a detection by the security monitoring team. Unfortunately, this action evaded detection by the security team. What was the punishment? After the breach, the data protection regulator fined Bupa Insurance Services over $200,000 for failing to stop an employee from stealing. Think of these like any other breaches, the disruption to business operations, the lack of customers' trust, and above all the reputation damage to the company.

Don't wait! We know that the threat landscape keeps evolving with new attack vectors and attack techniques, giving you even more reasons to evaluate your current cybersecurity solutions.

What to Expect

Our cybersecurity trusted advisors are available to help provide the necessary visibility across your entire network infrastructure and thus allowing for proactive threat detection and improved incident identification, robust investigation, and rapid resolution.

Additionally, our subject matter experts will help and guide your team to implement cost-saving measures to proactively identify, mitigate, and remediate security threats and potential attacks. In other words, the knowledge gained can be used to inform decisions regarding the enforcement of policy and best practices to stay protected against future attacks to a large extent.

Response, Impact, Root Cause Analysis, **and Lessons Learned**

Want to discuss the response, real impact, root cause analysis, and lessons learned from this attack, and count on us to have the discussion tailored to your needs? Then make a decision now!

The team of cybersecurity experts from AbriteLogic Solutions is available to offer a FREE half-hour consultation to discuss the relevant details along with the security implications it may possibly have on your organization.

EMAIL ACCOUNT COMPROMISE AND THE REPERCUSSIONS

Synopsis of the Attack

Ambry Genetics — a California-based genetic testing lab — revealed back in April of 2020 that an email security breach had potentially compromised sensitive information pertaining to hundreds of thousands of patients. It was reported that hackers gained access to protected health information (PHI), personally identifiable information (PII), and other identifiers through an employee's email account.

Earlier that year, Ambry's security team noticed unauthorized access to one of their employee's email accounts and immediately initiated an investigation into the incident. While the company found no conclusive evidence of misuse and was unable to determine whether there was an unauthorized access to any particular information from the email account, it did not rule out the exposure of customer personal information.

As a proactive measure, the company offered its customers free identity monitoring services to affected individuals and reassures customers of the necessary steps taken to avoid any future incidents. However, the affected patients took legal action against Ambry, arguing the company failed in its duty to protect their information. Even though the company did not admit any wrongdoing, the leadership agreed to over $12 million class action settlement with over two hundred thousand patients who were impacted to address the allegation.

What to Expect

Our cybersecurity trusted advisors are available to help provide the necessary visibility across your entire network infrastructure and thus allowing for proactive threat detection and improved incident identification, robust investigation, and rapid resolution.

Additionally, our subject matter experts will help and guide your team to implement cost-saving measures to proactively identify, mitigate, and remediate security threats and potential attacks. In other words, the knowledge gained can be used to inform decisions regarding the enforcement of policy and best practices to stay protected against future attacks to a large extent.

Response, Impact, Root Cause Analysis, and Lessons Learned

Want to discuss the response, real impact, root cause analysis, and lessons learned from this attack, and count on us to have the discussion tailored to your needs? Then make a decision now!

The team of cybersecurity experts from AbriteLogic Solutions is available to offer a FREE half-hour consultation to discuss the relevant details along with the security implications it may possibly have on your organization.