Cloud based office solutions under increasing attack

Specialist insurer Beazley has reported that the number of business email compromises is accelerating, particularly for those organizations using Office 365, the popular cloud-based solution for Office applications and other Microsoft productivity services. These hack and malware breaches accounted for 13% of incidents reported to its Beazley Breach Response (BBR) Services team during the first quarter 2018. The three sectors most affected were financial services, healthcare and professional services.

In BBR Services' experience, these incidents are usually caused by an employee clicking on a link in a phishing email, HelpDesk message, or Microsoft survey. After clicking on the link, the employee is redirected to a legitimate-looking website and asked for email credentials. The hacker then harvests those credentials and logs into the mailbox undetected.

In general, email compromises are on the rise because they are relatively easy to carry out and threat actors are able to use the email accounts for a variety of purposes. Once in the mailbox, the attacker may run searches to steal personally identifiable information. The attacker may also steal bank information to send emails requesting fraudulent wire transfers. Additionally, attackers frequently search the inbox to determine what HR and benefits self-service portal the employer uses, and then requests a password reset for the user in that system. Once in the self-service portal, the attacker redirects the employee's paycheck to one of their accounts. Finally, the attacker often sends spam emails to all of the user's contacts in an attempt to get others to give up their credentials as well.

Katherine Keefe, global head of Beazley Breach Response Services, said: "The number of compromised email accounts is accelerating but simple steps such as frequently changing passwords, having dual-factor authentication and removing auto-forwarding or auto-delete rules can help reduce vulnerabilities. With privacy regulations becoming more stringent and the public demanding greater accountability for their personal data, it is more important than ever for organizations to secure their lines of defense."

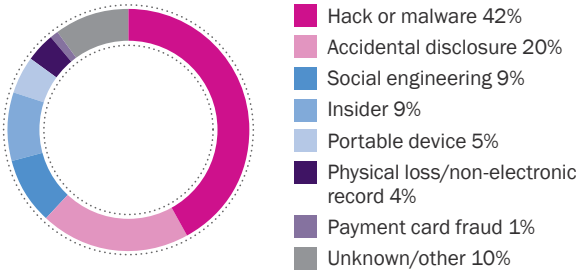
A large majority of breaches that the BBR Services team has worked on have involved Office 365. The default settings on Office 365 do not typically include the logging necessary to rule out a compromise of all emails in an inbox. Fortunately, BBR Services has identified several forensic partners that have created a tool to gain access to additional logs through Microsoft. With this additional insight, the number of affected individuals often drops, along with forensic and notification costs.

Organizations can protect themselves against these attacks by doing the following:

- Require two-factor authentication for access to Office 365.
- Microsoft provides a tool called Secure Score that can be used by anyone who has administrative privileges for an Office 365 subscription. It assists not just in analyzing, but also with implementing best practices regarding their Office 365 security.
- Enforce strong password policies. Educate employees about the risks of recycling passwords for different applications.
- Alert employees who have access to accounts payable systems or wire transfer payments about these types of scams.
- Train all employees to beware of phishing attempts.
- If you use cloud-based platforms, investigate what logging is available and make sure it is enabled. For instance, if you've migrated from on-premises Exchange to Office 365, audit your security settings, which are reset to default settings during migration. In Office 365, you must turn on audit logging in the Security & Compliance Center.
- Work with your cloud provider's technical team to determine what activities are logged and ensure you have the visibility you need, for the monitoring period you need.

The top two causes of data breaches reported to BBR Services in Q1 2018 were hack or malware (42%) and accidental disclosure (20%), consistent with incidents reported in Q4 2017. Social engineering and disclosure by insiders were the next highest cause of incident, each at 9%.

Causes of incident Q1 2018 (base 813)



CBSL548_US_04/18

Breaches by industry

Higher education

Hacking and malware incidents were up from Q4 2017 to 47% of the total number of incidents for higher education establishments. Also compared to Q4 2017, accidental disclosure recorded a 5 percentage point drop to 20% while social engineering plateaued at 9%.

Financial services

Over half (55%) of all data breach incidents reported to BBR Services in Q1 2018 were caused by hacking or malware, similar to the 53% recorded in Q4 2017. The number of social engineering incidents, which accounted for one in five breaches (20%) in Q4 2017, almost halved to 12% of the total in the quarter.

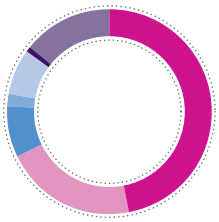
Healthcare

Accidental disclosure (29%) and hacking or malware (29%) endured as the most frequent causes of data breach in the healthcare sector in Q1 2018, at a combined 58% of the total. A slight reduction in the number of breaches caused by insiders from 19% in Q4 2017 to 15% in Q1 2018 is to be welcomed.

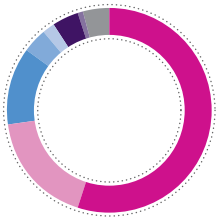
Professional services

There were two striking features of data breaches reported by professional services firms to BBR Services between Q4 2017 and Q1 2018: the number of breaches due to the loss of portable devices and due to accidental disclosure both doubled, while the number of social engineering incidents almost halved.

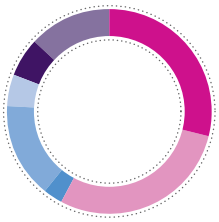
Higher Education Incidents, Q1 2018



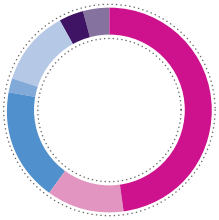
Financial Services Incidents, Q1 2018



Healthcare Incidents, Q1 2018



Professional Services Incidents, Q1 2018



Case study

When a Beazley policyholder employee received "strange emails" from another employee's email account, they reported it to their IT team. The emails were from a legitimate internal email address, but they were not being sent by the employee. The company acted immediately to contain the incident, by changing passwords, disconnecting the workstations from the network, putting the email into quarantine state, contacting their electronic medical records (EMR) vendor, and blocking the IP address that initiated the emails from the compromised account. They also contacted BBR Services to request assistance and guidance. BBR Services further advised the company to remove any auto-forward/auto-delete rules and, as the client used Microsoft Office 365 for email, explained the need for a forensic and legal review. Using a firm with Microsoft Office 365 capabilities to pull additional logs and determine which emails in the inbox had been accessed, they established that only 20 emails had been compromised and only three individuals needed to be notified of a breach of their personal information.

About Beazley Breach Response (BBR)

Beazley has managed thousands of data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches. Beazley's BBR Services team coordinates the expert forensic, legal, notification and credit monitoring services that clients need to satisfy all legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

beazley

www.beazley.com/bbr