Beazley Breach Solutions

Beazley Risk Management Intel

August 2019

Have you addressed the most common risks and vulnerabilities?

BBR Services is constantly looking to bring you insight on how to protect your organization on all fronts. We leverage our experience on the front lines of breach response to provide actionable guidance on the latest breach trends and emerging threats. Now we're excited to bring you real-world intelligence from the pre-breach arena. Our affiliated cybersecurity company, Lodestone Security, works with organizations every day to assess and improve their cybersecurity posture. Based on Lodestone's actual aggregated findings from recent engagements, we bring you the risk areas most small and medium businesses fail to address, and the top security vulnerabilities you can remediate for quick wins.

Top 5 risks from risk assessments

1. No vulnerability assessment/penetration testing/vulnerability management program in place (Either Lodestone's scans were the first scans performed or minimal scan was performed in distant past; as a result, there was no proactive plan to periodically identify and remediate vulnerabilities)

- See Pre-breach services for more information on services

2. No Security incident response program in place (Either no formal documentation and program was in place, or Lodestone's incident response plan development was the first step towards establishing the program)

- See resources at Incident response plans

3. Weak logging and monitoring capability (only basic logging turned on; providing little-to-no visibility into actual security events. Where logging events were available, periodic/continuous monitoring of event alerts (response capability) did not appear to be in place)

- See our recent webinar Cybercrime Spotlight: Logging and Monitoring

4. Administrative privileges were not restricted (non-IT users and third parties were provided full administrative privileges on workstations and servers)

- See *Manage User Accounts and Access* in the Lodestone Cybersecurity Primer for SMBs

5. IT disaster recovery plan/capability not formally established (companies were shown to be reliant on systems or cloud apps without having any fail-over capability implemented in the event of disruptive issues or IT service outages. Where cloud applications were used, the cloud vendors did not have guarantees for availability in place (SLAs))

- See resources at Business continuity planning and Privacy Builder: Vendor Management, as well as our webinars Cybercrime Spotlight: Effective Backup Strategies and Cybercrime Spotlight: Cloud cybersecurity

Top 5 vulnerabilities observed

Talk to your IT team or service provider to make sure you're addressing these common vulnerabilities.

1. MS17-10 (ETERNALBLUE) is still an exploitable vulnerability for about half of our client base. BlueKeep Remote Desktop (RDP) vulnerability has been identified periodically.

2. HP System Management and Intel Management Engine, which are used to remotely administer servers (like an online BIOS), are often unpatched.

3. Local shared administrative passwords allowed Lodestone to pivot across the network into multiple machines, increasing the vulnerability impact of cybersecurity exposures.

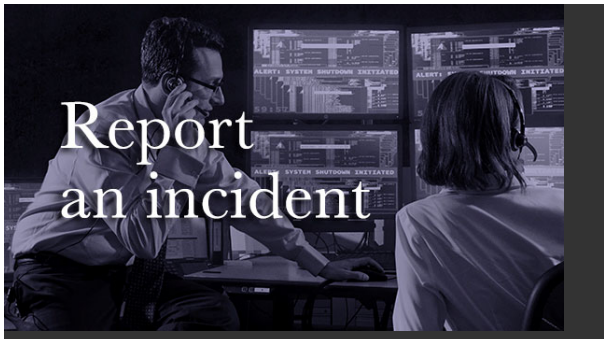
4. Vulnerabilities in and misconfigurations of SSL/TLS are abundant. Severity ranges from moderate to high impact, and even critical impact when associated with legacy protocols vulnerable to attacks like Sweet32, POODLE, Beast.

5. Exposure of administrative interfaces to the Internet (e.g., VoIP system, solar power array, MSP remote endpoint management tool from MSP that used default usernames and passwords).

Lodestone is a wholly owned subsidiary of Beazley plc and does not provide insurance services. Beazley does not share insured-specific information with Lodestone. Information you provide to Lodestone and any engagement findings are shared only between your organization and Lodestone. Information supplied by Lodestone for this article was provided on a de-identified, aggregate basis.

If you haven't registered for our risk management website yet, visit beazleybreachsolutions.com and register using your activation code dOqmyO.

We want to hear from you
Email us at bbrservices@beazley.com
with your risk management questions or suggestions.



You should notify Beazley as soon as you suspect that personally identifiable or confidential data for which you are responsible might have been compromised. The sooner you notify us about a potential data breach, the more our BBR Services team can do to help.

Email: bbr.claims@beazley.com

Phone: 866 567 8570 (toll-free hotline)

Online: Incident response form

beazley

beautifully designed insurance

This alert is part of the risk management services provided with your Beazley Breach Response ("BBR") insurance policy.

BZEM049_US_08/19