Critical Security Updates Released by Leading Software and Technology Companies

By: Linda Perkins
Cyber Law and Data Protection Alert
4.20.17

The week of April 17, 2017 is proving to be a critical week for technology security updates. The United States Computer Emergency Readiness Team (US-CERT), which operates under the Department of Homeland Security, tracks daily announcements of security updates released by software and technology companies. This week has seen a significant uptick across the board for critical and high-to-medium security updates, patches and alerts from many companies including Google, Apple, Microsoft, Cisco, Oracle, Adobe, Apache and VM Ware. These are significant updates and should not be ignored.

We encourage our clients to check for and install security updates on a daily basis for at least the next few weeks until the need for "critical" or "high" impact security updates, as identified by your software, technology and internet providers, begins to subside. Daily checks for security updates will also help to ensure that critical patches and updates are not missed during a hectic day.

We also encourage our clients to remind their employees to be vigilant in updating any personal devices they may use, especially if those devices connect to business or workplace servers or network systems in any manner.

US-CERT regularly updates its Current Activity webpage as new advisories and alerts are issued. This information is made available to the public and business owners in an effort to keep them informed of current online threats. White and Williams monitors US-CERT alerts in an effort to keep its clients well informed when critical threats emerge.

In terms of best practices, businesses may elect to designate a specific individual to monitor the US-CERT webpage so that your company has critical information about internet security in a timely manner. Email alerts can be set up so that designated subscribers are notified as the threat environment changes.

White and Williams reminds its clients that internet security remains a critical component of any workplace policy or business operation plan. If you have questions or would like to discuss your policies and plans related to data privacy and cybersecurity, please contact Josh Mooney (mooneyj@whiteandwilliams.com; 215.864.6345), Jay Shapiro (shapiroj@whiteandwilliams.com; 212.714.3063) or Linda Perkins (perkinsl@whiteandwilliams.com; 215.864.6866).

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only and you are urged to consult a lawyer concerning your own situation and legal questions.