Cyber Insurance, Privacy and Data Security Newsletter - October 2014

Published 23 October 2014

Many organisations were "shell-shocked" this month as a vulnerability affecting a widely used Unix shell revealed that a wide range of operating systems could be exploited by hackers.

The Shellshock vulnerability arises out of the GNU Bourne Again Shell ("Bash"), a command-line shell on which many commonly used operating systems are built. The vulnerability can be used to attack devices that use Bash to execute scripts.

This vulnerability is concerning because of the multiple weak-spots it opens up to potential attackers. For example, the simple task of loading a website gives attackers the opportunity to exploit the vulnerability if the server handling your website request uses Bash commands to access the information you requested. In fact, many of the systems we use on a daily basis are vulnerable to such attacks, if a patch hasn't been put in place.

The Shellshock revelations were particularly alarming because it demonstrates that, however secure an organisation might think it is, there are still unknown vulnerabilities which undermine the security of the very foundations of IT architecture.

The effect of such systemic risks (and their sudden publication) could lead to multiple incidents across policies. For insurers and reinsurers, this raises questions around the aggregation of those losses; and, whether the "proximate cause" of those losses is the vulnerability itself or those who choose to exploit it.

The ICO's guidance earlier this year ("learning from the mistakes of others") highlighted the risks of failing to keep security software up to date by "patching". Following Shellshock, most software providers issued patches for their systems and it falls to companies to put those patches into effect. The ICO warned businesses that they needed to "to be aware of this flaw and need to be monitoring what they can do to address it. Ignoring the problem could leave them open to a serious data breach and ultimately, enforcement action".

Well known systemic vulnerabilities such as Bash raise questions as to whether cyber underwriters should take a similar strict approach as the ICO and either seek to exclude known vulnerabilities within a certain period of time, or at least incorporate them into their underwriting criteria at renewal.

For DAC Beachcroft cyber updates, please follow us at **@legallnutt** and @hillegal1970.

For DAC Beachcroft privacy updates, please follows us at @DACBprivacy.

Authors

Rhiannon Webster
London - Walbrook
+44 (0)20 7894 6577
rwebster@dacbeachcroft.com

Patrick Hill
London - Walbrook
+44 (0)20 7894 6930
phill@dacbeachcroft.com

Hans Allnutt
London - Walbrook
+44 (0) 20 7894 6925
hallnutt@dacbeachcroft.com