Cyber attack forces Code Spaces out of business – a wake-up call for the boardroom, says IT Governance

An organisation’s cyber resilience is the critical survival factor as the severity and frequency of attacks increases

ELY , UK, June 23, 2014 /EINPresswire.com/ -- Code Spaces, the code hosting and software collaboration platform, was forced to cease trading for an indefinite time after a hacker deleted the company’s data and backups.

In what seems to be the first example of a large company being ‘knocked out’ of business due to a cyber attack, Code Spaces apologised in a statement on their website saying that, “at this point in time we have no alternative but to cease trading and concentrate on supporting our affected customers in exporting any remaining data they have left with us.”

Geraint Williams, senior consultant at IT security firm IT Governance, says,
“The news that another large company has been breached is not the real surprise, as we have seen this happen many times over the last year. The real shock comes from the fact that the severity of the attack has forced Code Spaces out of business and revealed serious gaps in their incident response plan.

“During incident response an organisation should always be able to pull the plug on Internet access to servers to prevent remote access. In this case, however, the infrastructure attacked was not owned and operated by Code Spaces but part of a Cloud environment where the ability to isolate a server from remote control is a lot more difficult. Incident response procedures must take into account host environments.”

From the statement that Code Spaces have given, it is apparent that the company did not use a robust two-factor authentication scheme for the control panel even though the hosting service provider supported such authentication schemes. The backup policy did not provide enough protection, and their business continuity and disaster recovery procedures were not robust.

Williams continues, “The attack on Code Spaces was an extortion attempt. It is not clear from the Code Spaces statement when the attacker gained access to the Amazon EC2 control panel. What is known is that a DDoS attack was launched and a blackmail attempt was initiated with the attacker using a Hotmail account. Code Spaces currently have no indication that a malicious insider was involved.

“It also appears that password compromise was the key factor. The secure use of strong passwords must be part of the culture of an organisation. Staff awareness combined with strong, computer-generated, random passwords, in conjunction with technology such as passwords vaults and two-factor authentication would mitigate attacks on passwords.”

The IT Governance 2014 Boardroom Cyber Watch Survey has revealed that both the boardroom and

IT departments may be too complacent when it comes to preparing for cyber attacks. While 73% of respondents claim they are capable of repelling cyber attacks, almost 36% of respondents believe their company was probably subject to undetected cyber attack in the past year, and almost 21% did not know. Such high percentages of uncertainty about whether an attack has occurred, or not, indicates very clearly that, in many cases, the organisation’s belief that they are secure against attack is likely to be unfounded and will expose them to the sort of existential threat that forced Code Spaces out of business.

Williams goes on to say, “This type of attack could be conducted against a large number of organisations. Use of the Cloud is not a replacement for a well thought-out and implemented business continuity and disaster recovery policy. Organisations are not doing enough to protect sensitive data.”

“This attack also demonstrates that an organisation’s cyber resilience is now the critical survival factor – its ability to recover quickly once an attack has taken place. I would call this a wake-up call for both the boardroom and senior management who are unequivocally responsible for business continuity.”

More information about cyber resilience is available form IT Governance at: www.itgovernance.co.uk/cybersecurity-training.aspx.

- Ends -

NOTES TO EDITORS:

IT Governance Ltd is the single-source provider for books, tools, training and consultancy for IT governance, risk management and compliance. The company is a leading authority on cyber security and IT governance for business and the public sector. IT Governance is ‘non-geek’, approaching IT issues from a non-technology background and talking to management in its own language. The company’s customer base spans Europe, the Americas, the Middle East, South Africa and Asia. More information is available at: www.itgovernance.co.uk.

Desi Aleksandrova
IT Governance
+44 (0) 845 070 1750
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.