Matthew Shore
UP879148

Mitigating corporate information exposure on the web

Information exposure is a serious issue facing all corporations in the twenty-first century. Preventing information exposure is essential for maintaining the security of the information itself and those who are associated with the information. Hence Corporations take great steps to mitigate corporate information exposure on the web. This review covers the various methods which corporations can employ to reduce their information exposure on the web.

Firewalls are an essential part of how corporations mitigate information exposure on the web. The primary purpose of a firewall is to prevent access from one network to another. Therefore companies are able to use firewalls to prevent unwanted pieces of data from gaining entry to their network and also to prevent unwanted pieces of data from leaving their network to the wider web. Firewalls in corporations are typically part of the information access policy that the corporation has in place. Firewalls are also managed by network engineers and the network administrator.

Firewall configurations in corporations also have to be regularly reviewed and independently audited to ensure that there are no unnecessary configurations on the firewall which might compromise the security of the network.

Google as well as many other large tech companies use a firewall to protect their corporations' information and data from exposure on the web. It is estimated that the largest tech corporations spend between 10 million and 15 million dollars annually on maintaining their information security systems and they spend much more than that on researching and improving them.

VPNs (virtual private networks) are another method which corporations use to mitigate their information exposure on the web. VPNs are very similar to firewalls in how they operate. Both a firewall and a VPN aim to protect your data and information when you are online. A VPN operates by tapping into a variety of dedicated connections using encryption protocols to create a virtual peer to peer connection. If someone who does not have the required permissions tries to access the transmitted data they will not be able to do anything with it because the data is encrypted.

The use of VPNs in corporations is on the rise as of 2017. The main reason for this is that a VPN is able to greatly reduce the risk of security breaches to the corporation and at the same time a VPN is very cost effective to use over other methods such as installing a corporate wide firewall.

Proxy servers are another method which corporations use to mitigate their information exposure on the web. A proxy server essentially acts as the intermediary between the device trying to access the network and the network itself. This can significantly improve the security of a corporation's network from potential information exposure by keeping the internal network structure that the corporation uses secret from the device accessing that it is communicating with by using network address translation. This makes the requests anonymous.

Use of proxy servers are often used side by side with firewalls

Another key aspect that corporations use to help mitigate against information exposure on the web is to train their employees who work within their company and network on Cyber Security. Corporations such as Google and Facebook regularly educate and train their staff on the potential risks that are involved when working on their network. This reduces the chance of an accidental leak of information from their network onto the web from someone inside of the corporation.

In addition to this corporations can also limit the amount of data which their employees have on a need to know basis. This can be done via permissions and user settings – limiting the amount of data and information that a particular account will have access to. Limiting the amount of people who have access to particular pieces of information reduces the chance of one of the people who has access accidentally or intentionally leaking the information out to the wider web. Hence mitigating the risk of exposure.

In conclusion corporations employ a wide range of methods to mitigate their information exposure to the web. These include the implementation and use of Firewalls, Proxy Servers, Virtual Private Networks and training and informing their staff about the issues regarding cyber security.

Matthew Shore
UP879148

Bibliography:

Basic Principles and Some Implications, B. Douglas Blansit, published 04/09/2009, accessed 30/10/2017 goo.gl/RTq7JM

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Douglas J. Landoll, published 2006 by Auerbach Publications, accessed 30/10/2017, goo.gl/DYVrLu

Global supply chain design considerations: Mitigating product safety and security risks, Cheri Speier, Judith M Whipple, David J Closs and Douglas Voss, published November 2011, accessed 30/10/2017, goo.gl/VI3b99

Control Systems Cyber Security: Defence in Depth Strategies, David Kupiers and Mark Fabro, published May 2006, accessed 02/11/2017, https://goo.gl/AdbX3z

Corporate information security management, Ruth C. Mitchell, Rita Marcella and Graeme Baxter, accessed 02/11/2017, https://goo.gl/kpuw23

Other websites and research:

Sans Technology Institute, Top 5 Firewall Leaks, Chris Brenton, accessed 30/10/2017, https://www.sans.edu/cyber-research/security-laboratory/article/top-firewall-leaks

Reducing your exposure to cyber-attack, National Cyber Security Centre, published 10/12/2015, accessed 30/10/2017, goo.gl/XMGs3U

Six network security checks to mitigate the risk of data security breaches, Information age, published 28/05/2015, accessed 30/10/2017 https://goo.gl/KuBNuy

Five ways your company can benefit from using a VPN, Computer World, published 06/04/2017, accessed 01/11/2017, https://goo.gl/VvtsCr

How much do companies spend for cybersecurity?, Quora, published 28/12/2016, accessed 01/11/2017, https://goo.gl/gUK9Me

Google's CIO explains the challenge of keeping data secure, thenextweb, published 12/03/2013, accessed 02/11/2017, https://goo.gl/nyDLtN

What do companies like Apple, Google and Facebook do to prevent hacking, Quora, published 27/10/2015, accessed 2/11/2017, https://goo.gl/kxJkqE

RSAC 2017: BeyondCorp – How Google protects it corporate security, duo, published 21/02/2017, accessed 02/11/2017, https://goo.gl/gc1A8Z

Five reasons your company should use proxy servers, cmswire, RJ Prego, Published 20/06/2016, accessed 02/11/2017, https://goo.gl/xpZhPj

The basics of using a proxy server for privacy and security, Partick Lambert, techrepublic, published 4/12/2012, accessed 02/11/2017, https://goo.gl/RoRavr