Mitigating corporate information exposure on the web

UP877962

With the widespread use of databases and the growing popularity of cloud computing more information is stored on the web than ever before, however these benefits come at a cost and the web also opens corporations up to a whole new range of threats. Considering these companies hold personal and often sensitive information about people who use their services,this paper will examine what can be done to mitigate the risks.
There are several widely accepted procedures that corporations can take to mitigate threats to their systems and prevent information exposure on the web.*(National cyber security centre, N/a*) Starting with establishing network boundary defences such as web filtering and content checking software, these monitor and restrict traffic from outside networks automatically blocking suspicious websites which could potentially be hiding malicious software or links within. It can also be beneficial to use these systems to block access to, for example social media sites during work hours thereby removing another potential vector for information loss.

Another good practice for corporations to have is some form of firewall running on their system, there are several different levels of firewall which can be applied at either a system level or also on individual user machines.This software creates a virtual barrier of code around your network or on individual computers that all traffic must pass through and it will automatically cross check this traffic against known blacklists. Malware protection otherwise known as Antivirus software is another program that runs on individual computers on your systems and is designed to constantly scan computers and check software and files against known databases of malicious software. It is important that is kept up to date and patched as needed as new exploits are being discovered on a daily basis,*(Shruthi prabhakar, 2017*) and because any software loaded directly onto individual machines can bypass a corporation's perimeter network defences making it far easier for the attacker to go undetected.

It is highly recommended to ensure any software companies/corporations may be running such as operating systems are up to date and still supported by the manufacturer and that this software is fully patched and updated whenever required to prevent known exploits being used against you. A good example of this being the recent ransomware attacks on the NHS that managed to spread across their whole network and caused massive disruption for several days, it was their use of the outdated and (at that point) no longer supported microsoft windows XP that made this attack so damaging. *(Nao.org.uk, 2017)*

Computers on your network should also be configured to block the use of autorun features for CD and USB devices to prevent individual users either inadvertently or deliberately installing malicious software directly onto individual machines within networks thus bypassing the above mentioned network defences. Individual users of your systems should only have the minimal level of access that is necessary for them to carry out their work efficiently and to the standard required. A strict password policy should be in place requiring regular changes and passwords used should be in a mixed format using upper and lowercase letters as well as numbers and symbols. Passwords should never be written down or based on some form of personal information that may be guessed or found out through tactics such as trawling social media or other more sophisticated forms of social engineering.*(Joseph a casier & B dawn medlin, 2006)*

Employees should be made aware of the precautions they should take in the workplace such as never opening unknown links in emails or if access is allowed on external websites.
Any information held by corporations should be assessed and stored based on how sensitive it is with sensitive data such as personal and financial information completely ring fenced from your external facing systems. In most modern countries there are very strict laws which govern how data is used and held with some significant fines having been issued in the past when there have been breaches to corporate systems and data has been stolen so it is essential that all necessary legal obligations are met. High level encryption protocols should be used to ensure should any data that may be stolen will at least not be easily readable and thus turned into information that may be of use to criminals or others with an interest in your systems. Critical system infrastructure such as servers should also be contained within locked rooms with only those staff who need physical access such as system administrators able to enter.

In the event that a corporation's system defences do become breached and it is quite widely accepted within the internet security industry that there is no such thing as a secure system*(Lorrie faith cranor, & Simson garfinkel, 2005, pretext)* corporations need to ensure that they have a robust contingency plan in place to minimise damage or potential information loss, it is not an acceptable policy to just hope that your company or corporations already prepared network and user level defences will do their job. System administrators should have a good understanding of what is normal for their systems so that any intrusions may be detected at the earliest possible stage, as the longer an attacker has access to your systems the harder they will be to detect and the more opportunity they will have to cause damage or steal sensitive information.

In conclusion mitigating corporate information loss or exposure on the web needs an in depth multi pronged approach which minimises the potential attack vectors at every access point throughout your systems from point of internet access down to individual users access. System administrators need to be fully aware of what constitutes normal usage and traffic on your systems and safeguards must be in place for when a breach does occur.

References

Joseph a casier, J. .A. .C & B dawn medlin, B. .D. .M. (2006). Password Security: An Empirical Investigation into E-Commerce Passwords and their Crack Times. *Information Systems Security*, 15(6), 45-55.
In-text citation: (Joseph a casier & B dawn medlin, 2006)

Lorrie faith cranor, , L.F.C & Simson garfinkel, S.G.(2005). *Security and Usability: Designing Secure Systems that People Can Use*. : "O'Reilly Media, Inc".
In-text citation: (Lorrie faith cranor, & Simson garfinkel, 2005)

Nao.org.uk. (2017). *National Audit Office*. Retrieved 19 October, 2017, from https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
In-text citation: (Nao.org.uk, 2017)

National cyber security centre. (N/a). *National Cyber Security Centre*. Retrieved 17 October, 2017, from https://www.ncsc.gov.uk
In-text citation: (National cyber security centre, N/a)

Shruthi prabhakar, S.P. (2017). NETWORK SECURITY IN DIGITALIZATION: ATTACKS AND DEFENCE. *INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS*, 5(5), 46-52.
In-text citation: (Shruthi prabhakar, 2017)