Block or not: should you monitor employees' content consumption?

By Andrew Wilson

12 Dec 2017

Talk of monitoring and blocking employee access to certain types of internet content might sound like draconian management measures. After all, we're all adults in the workplace and we shouldn't need to be told what we can and can't look at on the internet, right? Not exactly. There are many reasons why businesses large and small would choose to block access to various categories of content, ranging from legal concerns to productivity considerations and cybersecurity risks.

© Rabia Elif Aksoy – 123RF.com

In South Africa, certain types of pornography and gambling sites are illegal. Piracy (downloading illegal copies of movies and other copyrighted content) is also outlawed – all of which expose a company to legal risks when an employee uses corporate resources to access such content. Other types of content that companies should block include sites known for malware and phishing, for obvious reasons. So how can companies prevent their enterprise resources from being used to access and consume such undesirable content? This would appear to be a perplexing question to answer, especially when faced with ever-growing pressure to allow the Bring Your Own Device (BYOD) movement free rein in the workplace.

With employees demanding unhampered access to the internet and corporate infrastructure across all of their devices, often remotely, how can organisations prevent these connections from being abused? Fortunately, thanks to developments in Artificial Intelligence (AI) and technology, not only is it a possibility, but it can be done without having to resort to watchdog tactics. In short, technology has evolved to the point where it can now be used to empower organisations to allow their employees to self-manage their online content consumption, while securing their connections and ensuring the security of the enterprise networks.

Blocking is old-school

Traditional controls usually look at blocking certain sites and there are many companies that still do not allow access to Facebook and YouTube for employees. This approach is completely outdated and often has exactly the opposite effect than intended. If access to sites like Facebook and YouTube is restricted at work, employees will simply get creative. They'll use their personal devices to connect directly, which will result in higher 3G mobile connectivity bills. However, regardless of the

cost and admin associated with mobile connectivity, from a security perspective it's even more problematic. This is due to the fact that these devices that make use of 3G connectivity often don't have the security protection against malware and/or phishing sites, or even exposure to ransomware, thereby putting the company at greater risk.

Block-and-deny approaches to internet content is regarded by most as 'old school' and is often counterproductive. Not only does this approach result in staff unhappiness but as social media becomes a legitimate part of the organisation, businesses can no longer just simply block sites that are labeled as 'unproductive'. To this end, it is advisable not to block access but rather to manage it. This means looking at solutions that provide 'clean internet'.

If not blocking, then what?

What happens once an organisation has visibility of all the connections taking place on their network? Good things. Visibility is great for cyber security as it's now possible to measure, manage and control connections in order to minimise risk to the company. Luckily businesses don't have to attain this visibility on their own as there are already technology providers out there, ready to assist. These intelligent network and cyber security services are subscription-based and deliver easy-to-understand reporting functionality into every aspect of the network. Inexpensive and uncomplicated, all that an organisation needs to use such services is the correct hardware compatible with certain analytics software. This software makes use of big data to comb network activity and connectivity logs for anomalies to identify all types of content that organisations would want to keep their employees from engaging with: from malware, ransomware, and phishing attempts, to the consumption of explicit, illegal and pirated content. Once these connections have been identified, they can be appropriately managed in line with corporate policy.

Aside from ensuring the integrity of connections within the network, once visibility is enabled it becomes possible to implement self-management of employee access to content. How does this work? Technological solutions that enable this kind of visibility into network and user activity make it possible to report on their online activity. Where an organisation is having productivity concerns with an employee, it's possible to see exactly how much time that employee spends online, and exactly how they're spending it. Rather than this situation devolving into a confrontational disciplinary hearing, an employee is far more likely to self-correct behaviour once presented with their user report. In our experience, 99.9% of internet abuse in the workplace disappears once the users feel that the anonymity of the internet has been removed simply by introducing the feeling that someone else might be watching.

The answer is always simple

When it comes to abuse management of enterprise resources, as well as maintaining security in an ever-changing technological space, the answers to the tough questions are usually the simple ones. It is for this reason that businesses should take a step back and look at the bigger picture: by securing all connections (especially those on personal devices) it becomes possible to manage and enforce corporate content policies without resorting to draconian measures.

ABOUT THE AUTHOR

Andrew Wilson is the CEO of LucidView.

For more, visit: https://www.bizcommunity.com