How CISOs can maintain corporate privacy

By Doros Hadjizenonos

6 Nov 2018

Today's workforce is increasingly comprised of millennials and other tech-savvy individuals that are accustomed to using technology in every aspect of their lives. As new technology emerges, this group of employees expects a seamless user experience across devices and locations, using personal applications and devices at work and vice versa.

Source: pixabay.com

However, many times these employees are not considering the cyber risks that may accompany bringing new technology into the corporate environment. The resulting security challenges have become a major pain point for CISOs.

In addition to maintaining perimeter defences, monitoring threat intelligence, and the other daily responsibilities required to stop cybercriminals from accessing the network via zero-day threats and vulnerabilities, CISOs must now also consider all of the ways cybercriminals might leverage the tools and behaviours of their employees to gain access to the network.

The expanding user attack surface

Insider threats have become a key concern for CISOs and security teams. These threats do not only refer to employees intentionally attacking their organisation. More often, these threats come down to employee negligence and the use of technologies without thought being put into related cybersecurity best practices. As a result, today in 2018, 51% of organisations worry about security risk due to human error.

Unfortunately, insider threats will only continue to increase as the human attack surface grows. It's predicted that there will be six billion internet users by 2022. As a result, some cybercriminals have begun turning their focus to leveraging and exploiting human access, rather than attacking machines.

Why are CIOs and CISOs positions becoming more challenging?

Pieter Engelbrecht 31 Oct 2018

To minimize risk, CISOs and security teams will have to be aware of the devices and tools being used by employees and deploy the necessary controls to secure them.

Maintaining privacy and security with emerging technology

In particular, there are five common and emerging technologies, trends, and behaviours that CISOs must pay attention to.

1. Reusing passwords

People commonly have a host of accounts on different platforms and apps. Many use the same login credentials on all of them, regardless of whether they are personal or corporate accounts. This is a significant issue. If one account is hacked, cybercriminals can use credential stuffing to leverage one password for access to other accounts. The issue is especially exacerbated by cloud use – if the same password is used across all cloud accounts, then when one is hacked, they all are.

To combat this, security teams must promote the use of new passwords, especially for corporate accounts, and at the same time, limit access to areas of the network not required of the employee. This can be done with identity and access management solutions that enforce two-factor authentication, password management software so users can implement a more sophisticated password strategy without constantly losing track of passwords, and internal segmentation firewalls that restrict access to sensitive parts of the network.

2. Shadow IT

When employees use technology not reviewed by IT teams, it can lead to data leakage, vulnerabilities, and non-compliance as they move sensitive corporate information beyond approved programs and networks. CISOs and security teams must be aware of what devices and applications are being used within the network at all times. Using endpoint protection and web application firewalls allow security teams to minimize the risk posed by these insiders by discovering endpoints and applications on the network and then identifying and segmenting those at risk.

Basic cyber hygiene practices that go a long way

Doros Hadjizenonos 9 Oct 2018

3. Remote connections

Working remotely is becoming more common, with employees going online from home, coffee shops, or on the road. While this can help productivity and efficiency, CISOs must be sure that these devices are connecting from secure access points. When using public WIFI, cybercriminals can intercept data running between the end user and the organization.

CISOs can minimize this risk by encouraging the use of VPNs and deploying wireless management solutions.

4. Email and phishing scams

While not new, this remains one of the most common attacks that cybercriminals use to target people, as nearly everyone uses email on a regular basis. With phishing scams, users receive an email from a seemingly trustworthy source, such as their bank, a co-worker, etc. These emails will typically ask the user to submit their credentials or click a link, which results in stolen passwords and/or downloading malware that infects the device. To minimize the chances of a phishing attack infecting the network, CISOs should implement controls such as secure email gateways.

5. Social Media

Social accounts are a common avenue for cybercriminals to distribute malicious links, or gather personal data that can be used to create more targeted attacks. CISOs should implement a strong social media policy, and discourage employees from accepting friend requests and message requests from strangers, especially if they are encouraged to click on a link while on the corporate network. Security teams should ensure they have antimalware and firewall solutions in place. They should also train employees to recognize social engineering schemes that seek to steal their data to access corporate networks and accounts.

AI, machine learning boost cybersecurity

8 Oct 2018

While CISOs often already own many of the tools needed to minimize the risk of these trends, it is equally important that they use them in a unified manner rather than deploying disparate, isolated solutions. Integration and automation between secure email gateways, firewalls, endpoint protections, WAFs, access management, and more provide a holistic view into activity across the network, allowing teams to quickly detect potentially-threatening behaviour or actions and then respond in a coordinated and holistic fashion.

Final Thoughts

The trends and technologies being adopted by employees and then brought into the corporate network are keeping security teams and CISOs on their toes when it comes to defence. These emerging technologies require new solutions and process to be deployed to stop seemingly harmless behaviours from turning into a network compromise of data breach. This can be done by staying aware of emerging technology trends and deploying integrated security solutions to minimise their risk.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...