Guide

Remote work, BYOD and corporate network security

Paweł Wałuszko 10.04.2020

It’s safe to say that BYOD (Bring Your Own Device) trend has never really caught on. Back in early 2010s numerous tech-oriented news outlets expected somewhat of a ‘how-we-conduct-business revolution’, but in reality, very few businesses actually embraced the model of employees using their personal devices for work purposes. Perhaps rightly so: personal computers are littered with random software, by definition are outside of control of the IT departments and, let’s not forget – there are software licensing issues.

However, the latest pandemic changed things up a bit. Some companies were forced to shut down permanently, as remote work is simply not a possibility in certain sectors. Others are trying to stay afloat, usually by allowing some of their workforce to work from home. It is at this point where numerous problems begin.

Ideally, a company prepared for ‘work from home’ situation would have a device ready for each employee. The laptop, tablet or a desktop computer would have proper software installed, security pre-configured and a secured VPN access built-in. All the employee would have to do, is to bring the machine home and plug it into their network, or any type of Internet access point.

Now, that would be ideal. However, for many businesses, things are far away from this setup. Even with the IT department coming in to work from 9 to 5, last-minute purchasing and setting up machines is a time-consuming task. For some companies, purchasing a new fleet of laptop computers could be flat-out prohibitive from a financial standpoint, as well. In the meantime, deadlines are approaching.

So, what do businesses do? Those who are not as fortunate to be in the best-case scenario, usually try to quickly remedy the situation by dusting off old, outdated computers laying around the office and giving them out to employees to work on, remotely. Others – usually small businesses – go as far as allowing their employees to utilize their personal machines for business use. After all, what difference does it make whether an Office document was edited on a business or a personal computer? A file is a file …right?

Employees are the main target

The fact that office employees have been a target for cyber-criminals is nothing new. However, given the current pandemic status, criminals have one more tool to work with: the informational chaos.

As Check Point’s *Global Threat Index* points out, since January there has been more than four thousand coronavirus-related domains registered. Out of these, three per-cent are considered flat-out malicious, and another five per cent, suspicious. This is very important, as although these single-digit numbers may appear insignificant, they represent fifty per cent rise in malicious domains being registered in comparison to the same period last year.

Moreover, sources indicate, phishing attacks are sharply on the rise, especially in locations, where coronavirus has been most prevalent – such as in Italy – where the number of phishing attacks has more than doubled. In fact, there has been so much misinformation and coronavirus-related cybersecurity attacks that the World Health Organization (WHO) resorted to publishing a warning on their website, outlining a list of scams, cyber-attacks and other ways of using social engineering to target vulnerable people, who simply want to find information relevant to their health.

This chaos is good news for cyber-criminals and presents a unique opportunity to even more so target individual employees. First, there is a higher chance that someone might click on a coronavirus-related link even on their business computer, therefore increasing the chance of malware entering a business network. Secondly, a number of employees will be working from home, which translates to numerous cyber-resilience measures being lowered or negatively impacted. Bingo!

How not to become a part of the statistic

It's important to point out that when it comes to cybersecurity, time is the worst advisor. Jumping on the BYOD and remote-work bandwagon can bring detrimental results to a business, as one improperly secured computer can wreak havoc in a business environment. (If one needs a reminder of what a simple piece of ransomware can do to a network, a good starting point is looking at the case of the City of Baltimore, which lost upwards $18.2 million in a single ransomware attack in 2019.) As such, the best advice, is to take it slow and secure each (preferably new) device appropriately.

The second advice would be to start monitoring the network – not only for vital statistics, but also unusual behaviors.

Software

There are numerous Network Monitoring Software (NMS) solutions out there. For those who favor the open-source approach to security and licensing, OpenNMS, Zabbix and Nagios are a good starting point. Although arduous to set up, these systems are quite extensive and can monitor nearly every aspect of the business network. Moreover, these systems are usually free.

Those who favor solid support and ease of deployment can look to ready-made solutions such as AdRem NetCrunch (Poland), Paessler PRTG (Germany) or Solarwinds NPM (United States).

When configuring such systems, it is worthwhile to pay attention to monitoring for script-like behaviors, i.e. events, which are not likely to be a result of a human being normally using a resource. For example, even a properly authenticated login, but happening far outside of standard business operating hours should raise our eyebrows. The same can be said for identical *access time* of dozens of files at a time (which can be an indication of malware mass-modifying files), or the same user logging in from two different IP addresses at once (which can be a symptom of password sharing or the password being stolen).

AI is here to help

As much as the NMS systems are extremely helpful in raising the administrator's awareness about what's going on inside their networks, there's one down-side to network monitoring, overall: it requires a sizable time investment on the behalf of the administrator. This is a direct result of how NMS systems tend to work: when a NMS notices an error (or a specified event), they usually trigger an alert. This alert is forwarded to the administrator, who usually has to manually check up on the situation. As one can imagine, informational overload can quickly settle in.

However, the latest hype – Artificial Intelligence (AI) – remedies this problem. When a behavioral monitoring solution backed by AI is deployed on the network, it quickly begins to learn how the network operates day-to-day. Moreover, AI automatically cross-references and correlates data from numerous data-sources available in the network, in order to make more accurate assessments. The direct result of this cross-referencing is superior security awareness through immediate, 24/7 behavioral monitoring. Best yet, certain AI-backed solutions can take immediate actions – such as running a script, disconnecting a device or blocking a user's account – as soon as it determines that there's a security risk. The administrator only has to intervene occasionally, when AI requests assistance.

To sum up

As a consequence of the current pandemic, BYOD and remote work are becoming a modus operandi for numerous businesses, which security-wise, might not necessarily be prepared for the situation. Given the information chaos and changes in the way the work is done, cybercriminals are ceasing on the opportunity and increasing their efforts, attacking companies in times of transformation. As such, perhaps the best advice is to resist time pressure and prepare appropriate back-end infrastructure, before jumping into the remote-work bandwagon.

From the back-end perspective, regardless of what cyber-resilience measures the business had already in-place, with the increasing amount of employees working remotely, there is a higher chance of these measures being weakened, or in some cases, failing to work all-together. Until we are absolutely certain that every end-point is secure, a network or behavioral

monitoring solution can significantly improve our cyber-resilience standpoint on top of already deployed efforts.

Rate the article:

5 / 5 (2 votes)

10.04.2020

Paweł Wałuszko

Business Development Manager i Ekspert ds. Bezpieczeństwa. Doświadczony menedżer w branży IT, który swoje doświadczenie zdobywał m.in. w Dolinie Krzemowej; entuzjasta oprogramowania open - source.

Gearing up for safe remote work

Search

To search, type and hit enter.

Recent Posts

Remote work, BYOD and corporate network security

Gearing up for safe remote work

How CEOs fall victim to hackers. The example of Jeff Bezos

Encrypted e-mail for private use. All you need to know

VPN for private use – a good idea?

Archives

April 2020
March 2020
February 2020
January 2020
December 2019
July 2019
June 2019
May 2019
April 2019
March 2019
January 2019
December 2018
November 2018
July 2018
June 2018
May 2018
April 2018
February 2018
May 2017