Guide

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

Paweł Wałuszko 24.02.2020

The 2013 Edward Snowden publicly confirmed something, which many of the IT experts were suspecting for years: the fact that an average computer makes for an excellent tool for spying on us. The media storm ensued.

Soon afterward, a flurry of privacy-oriented products and services popped up, as the society, in general, became more security conscious. While covering up a laptop webcam before 2013 might have been perceived as wearing a tin-foiled cap, after the Snowden's expose, a webcam privacy cover became a hit gadget at every IT-oriented conference. They were and still are given away by the thousands at any cybersecurity event. Meanwhile, some computer manufacturers go back to utilizing physical hardware switches for webcams – a feature that has not been common since the late 90s.

In a way, we can thank Edward Snowden for starting the debate. Today there is talk about privacy and cybersecurity, especially in business environments. We install anti-tracking browser extensions, frequently update our systems, utilize antimalware and antivirus programs. GDPR-wise – for those living in the EU – businesses train employees on how to properly handle sensitive data.

So far so good. However, when it comes to smartphones, many people tend to take a more laissez-faire approach: we install applications without vetting, we rarely check device-app permissions settings, we download and open files from e-mails without thinking about their origin. As usual, the list can go on.

Meanwhile, smartphones are extremely capable machines. The sheer feature set and the way that we use them makes the smartphone perhaps one of the best platforms to spy on someone or a company. High-definition cameras, body sensors, Wi-Fi, Bluetooth, and GSM connectivity, face recognition, applications for juggling personal and business life on a single device – all these make the mobile device the central hub for information. Moreover, in comparison with a standard laptop, we take it everywhere with us: from our office to the production halls.

CEOs also fall victim to attacks

The best example of why we shouldn't underestimate the security of mobile systems is the case concerning the CEO of the Amazon, Jeff Bezos.

In May 2018 Jeff received a message supposedly sent from the Crown Prince of Saudi Arabia, Mohammed bin Salman. According to the media reports, the message contained a video clip, which upon viewing, executed a few lines of additional code, allowing malware to install on the phone. Once on the device, the malware got privileged access to all resources and allowed hackers to examine all data, regardless of whether it would be business or private. With this simple method, the CEO of Amazon, one of the biggest IT-oriented companies in the world, got hacked.

A moment of carelessness can cost a lot

There's much speculation regarding the extent of damage the hack has caused. Some outlets point to the fact, that soon after the hack, Jeff and MacKenzie Bezos got divorced. We don't know whether Amazon sustained any business damage as well. However, given that the malware got access to all the phone's resources, including data from connected on-line accounts, we can assume that some business data also went public.

Meanwhile, not only Tier-1 CEOs are targeted. In business environments, data leaks happen quite frequently and incur sizable damages. According to Norton, just in the first quarter of 2019, 4 billion classified documents got leaked – a statistic, which is up 54% in comparison to the same time the year before. By the end of September 2019, this number rose to 9 billion and accounted for yet another 33% increase. Estimates by Juniper Research point to roughly 3 billion dollars as the overall business cost of cybercrime in 2019, and a single record leak is estimated by IBM to cost $150 on average.

As business owners, we are a part of the statistic. Considering how much data can be disclosed by compromising only one corporate email account, it is easy to estimate the real cost of such a leak in our company as well. In this sense, smartphones can be trouble: one device often handles numerous mailboxes, has access to internal communication tools and, in some cases, CRM or project management platforms.

Who are the hackers attacking

Given that even the CEO of Amazon got hacked, one may come into conclusion, that virtually every smartphone can be hacked – and all you have to do is have someone properly motivated to invest the time and effort. In a way, this is true. The fundamental question should be not whether it's possible to hack any phone – since we know that – but rather, who is worth such an investment.

The simplest answer is "the management", and the higher, the better.

According to the latest Verizon 2019 *Data Breach Investigations Report,* personnel with access to the most confidential information in a company are currently the main target of social engineering attacks. As Verizon points out, ***senior executives are 12 times more vulnerable to social engineering attacks and 9 times more susceptible to data leakage attacks*** in comparison to the same period last year.

The main reason for targeting high-level managers and CEOs are the financial benefits stemming from the access to sensitive data of the decision-makers. In comparison to other employees, managers have far more access to confidential data, posses the ability to move around the entire building or enterprise, sign contracts with contractors and often have administrator privileges on many crucial business platforms. Intellectual property theft is a lucrative business and there are many opportunities for monetization of ill-obtained data.

There's also the fact, that we tend to trust our mobile devices. As many platforms utilize passwords as a basic means of authentication, password recovery is possible through the smartphone. Moreover, two-step verification often by default relies on the smartphone as well: we receive a text message with a PIN to enter into a form. Thus a single device capable of receiving both e-mail and text messages is an ideal target for anyone looking to break in and circumvent two-step authentication systems, which are finally becoming commonplace.

Last, but not least, the form factor, albeit very ergonomic, is problematic as well. When designing a mobile application, developers have to make certain User Interface (UI) decisions. Small screens operated by a finger, rather than a more precise pointing device, cause developers to create apps which most efficiently utilize the screen space available. Consequently, large, most often used buttons appear in the foreground. The advanced, but less often utilized security functions are either completely removed from the app or hidden away in a menu, causing their usage to plummet.

How not to become a part of the statistic

We're not likely going to change the size of our smartphone screens for the sake of fitting in more advanced functionality buttons into the UI. We're also not likely to stop using our smartphones as a central hub of communication, both business and personal. After all, that's their main function. However, we don't have to completely write off security on these devices. A lock on the door does not guarantee resilience against a break-in, but it can make the process a lot more difficult. In some cases, it can deter an attack all-together. The same can be said about a proper approach to cybersecurity.

Remember, physical security is the best security

If you have two SIM cards – one for business and one for private use – it's best to simply use them on different phones, regardless of your device can accommodate them both at the same time. First of all, you won't be hampered by Mobile Device Management (MDM) policies, most likely put in place by your IT department. These policies can be very authoritative and dictate which applications you can install and use, as well as which settings and features will be available on your device. Secondly, if your private device becomes compromised, this situation will not jeopardize your business operations. With that in mind, never use a business password on a private device. Business data leaks are costly, and it's best not to be the cause of it.

Create barriers in terms of device functionality

If using two separate devices is out of the question, it's best to utilize a professionally-managed business mobile device, rather than BYOD ("Bring your own device"/personal) smartphone.

Unlike private devices, business smartphones undergo extensive security testing and security hardening process. This process entails securing software vulnerabilities and removing applications that may abuse access to smartphone's resources. In addition, MDM platforms enable application containerization, which means that business applications (theoretically) are separate from the rest of the phone and do not have access to the information and data of the user's private applications.

Let's tackle the issue of two-step authentication as well. If you are using the same device for receiving verification text messages and e-mail, it might be a good idea to look into alternative verification methods. A recently popular method is creating secure USB keys, which after being plugged in, can complete the second step of a two-factor authentication process. Voice verification thorough a land-line or a different device is a good alternative as well.

Invest in knowledge and apply good practices

Social engineering attacks are psychological attacks that exploit human nature and certain weaknesses in the decision-making process. People in managerial positions are more likely to work in a stressful environment, surrounded by deadlines and the constant need to juggle projects. This nature of managerial work contributes to making quick decisions, which can significantly impact one's cyber-resilience. For example, in Jeff Bezos' case, opening the unverified video file might have been preventable.

There's no golden pill against social engineering attacks. No technological solution can guarantee us 100% security, especially on mobile systems. Attacks on CEOs and managers are on the rise, and it's best to gear up and be informed. Regular audit of installed applications, awareness of application security standards and knowledge of what forms of attacks are currently used to hack smartphones is bound to bring far better results, than any ready-made solution.

Sources:

Norton. *Emerging Threats: 2019 data breaches: 4 billion records breached so far.*

RBS, *Q3 2019 Data Breach QuickView Report.*

Juniper Research. *The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024.*; IBM. Cost of a Data Breach Report, 2019.

Verizon. *2019 Data Breach Investigations Report.*

Rate the article:

★★★★★ 5 / 5 (1 vote)

24.02.2020