BIZCOMMUNITY

Security lessons learned from Sony's most notorious hack

By Carey van Vlaanderen

10 Feb 2015

In late November 2014, Sony was the victim of a cyber-attack that involved the release of stolen data, including yet-to-be-released films.

The hack not only destroyed data, but also impacted on present and former employees, exposing private emails and personal information such as social security numbers and salaries. The hackers called themselves, 'Guardian of Peace' or 'GOP' and demanded the cancellation of the planned release of the film, The Interview.

In the light of the attack, not only are we now seeing lawsuits, there is also the bigger issue of brand damage, and whilst Sony did manage to claw back some brand benefits by going ahead with the release of The Interview in the way that it did, the brand has still taken a hit.

Part of this is an historic issue, and the term systemic failure is not out of place here. Sony is an organisation that has a history of being attacked, and one that has failed to understand digital or cyberspace. Ten years ago, in 2005, Sony was responsible for the largest corporate spread of malware with the digital rights management that it put on music CDs, which was actually a stealthy root-kit that was installed on a lot of machines, and was then exploited by cyber-criminals. This was a black eye that showed a fundamental misunderstanding of the digital landscape, and it did not help that in 2011 its PlayStation network was hacked, with 77 million user accounts exposed.

Ways one can respond

There are several ways that one can respond to an issue like this; the first is to become the most excellent security that there is. The other strategy is to just live with the risk.

There were some comments made by Sony employees around the latest hack that there were known weaknesses in their security. We even know about some of the known weaknesses at Sony, because PriceWaterhouseCooper's audit from the second half of July showed that there was a significant chunk that was outside of the corporate security team's monitoring. This is something that we see all too often, where certain parts of an organisation go outside of the corporate security umbrella.

In light of the attack, here are three key lessons that businesses should take away from what may be the most notorious attack of this century thus far:

- Don't leave unencrypted audit reports in the executive email in-boxes: We tend to take email for granted and we think that

because it is corporate email it must be protected. The truth is, if the cybercriminals manage to get into the system, your emails are not safe. Yes, you may be encrypting your email on the server; however, if someone owns an account then it is not encrypted as the account owner gets to read that email. It seems like a simple rule, but it is a mistake that can lead to very nasty consequences. So, first and foremost, do not put anything in email that you may later regret saying or sharing (words, images, reports, etc.).

- Make your security awesome before you antagonise known hackers: This is not implying that we must give in to pressure from those who want to stifle our lives; however, the issue is that if you do not have a secure position from which to advocate beliefs, or say what you want, then you don't really have the freedom of speech that, in principle, you have. There are situations in the real world where your freedom of speech is limited by the neighbourhood that you are in when you think about saying something out loud to the world. The reality is that if you are antagonising people who are known to be active in hacking you have to first and foremost be very secure.

- A reminder that Hacktivism is here to stay: In security, we are fond of saying that the bank robber Willie Sutton was asked: "Why do you rob banks, Willy?" He replied: "Because that's where the money is." This is not actually true. Why did he rob banks? His actual words were, "Because I enjoyed it." This is the point of view of most hackers - it is because of the fun of it. The internet is fundamentally asymmetric. It is very difficult to stop people who are destructive. With DDos attacks you can bring a tremendous amount of resources to bear, just as a small group of people.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.
- 4 ways to manage the human threat to cybersecurity - 18 Jul 2023
- A cybercriminal's tricks and trades to get into your phone - 23 Mar 2018
- What is encryption, how does it work and why is it important? - 6 Mar 2017
- Five common security threats that demand attention - 9 Mar 2016
- Face 2016 with a proactive attitude of security awareness - 22 Jan 2016

View my profile and articles...