Behind the Scenes: Hollywood Encounters Cyber Security

Whenever you read the words ‘Hollywood’ and ‘Security’ in the same sentence, your mind probably wanders of in the direction of movies like*Die Hard 4.0* or *Swordfish* where uber-cool and suave hackers like Hugh Jackman trying to hack $9.5 Billion off the government from a computer with seven screens. Or if you are in the security business (or have the slightest interest in world news and technology) you would be aware of the Sony Pictures hack which sent the entire world into a tizzy and this according to some was the primary reason why Sony Pictures Co-Chairman Amy Pascal stepped down .

But the relationship between Hollywood and Cyber Security these days has far transcended the traditional connotation of blockbuster sensationalism. Hollywood is getting far more serious about cyber security and its impact – both on the global landscape and within the film industry in itself.

It is not just about the movies Hollywood makes; cyber threats have impacted the very foundations of how the industry works. Movie production houses have now woken up and are becoming highly cognizant of the dangers posed by confidential/ sensitive information falling into the wrong hands. Even till a couple of years ago, movie scripts were protected by watermarks or printed on specialty papers and all that production houses had to worry about was physical photocopies being taken of the script or similar sensitive documents. However, the shift to digitization and the advent of smart phones has exposed these production houses to internal as well as external threats. Cyber hackers are constantly knocking at their doors in search of the slightest security loophole which could be leveraged to breach the network. Either motivated by curiosity about how their next movie will pan out (James Bond Spectre script leaked) or sometimes politically motivated (like the Sony Pictures Hack), these hackers are not looking for financial gains. Nevertheless, the resulting financial impact on the movie industry is huge.

Today, hackers are not the biggest security challenge the industry faces – they are the internal employees or crew. Every document and communication pertaining to the movie is now in digital format and a large chunk of the movie crew has the movie script either on their iPads or smartphones. While companies cannot really avoid any of the above mentioned changes, they can surely implement controls which can ensure proper security

So what measures can the industry adopt to thwart off these attacks and ensure complete protection of sensitive information?

An ‘Air-Gap’ Network – Taking a cue from the critical infrastructure industry, production houses could adopt the concept of air-gaps to protect their sensitive data. Air-Gap is a concept in which sensitive information resides on a network which is physically isolated from the larger network so that even if that network is compromised, the sensitive data is still safe. The script of The Interview or James Bond’s Spectre would have been untouched had Sony Pictures used air-gaps.

Suitable Access Governance – Determining who can access, edit, download, and print documents pertaining to the movie script or budget details is extremely important. Role-Based Access and Context-Aware Access Governance would go a long way in protecting unauthorized usage and data being accessed by adversaries. The controls should be such that if the movie script is accessed by the spot-boy (role-based) or by someone from Romania (context-aware), it immediately sends out alerts and ask for additional authentication requirements.

Data Encryption – This is a tried and tested way of protecting sensitive information. In this method, data is encrypted so that people who do not have the proper access rights or the correct password will only be able to see gibberish. This is relevant because generally movie scripts are shared with the key actors and crew members and there are high chances of it falling in the wrong hands. However an encrypted file can only be accessed by people having the right passwords and those without the password will see gibberish.

Security Awareness – In most cases, breaches happen due to the lack of awareness and carelessness of employees. Employees need to be properly trained about the basic security processes and controls they need to adopt at an individual level. Elementary do's and dont's like not clicking on email links or setting strong passwords should be mandated across the organization. It is surprising to note how many networks have been breached due to employees not following security fundamentals.

Cyber-attacks are constantly evolving and we need to ensure that we evolve at a faster pace. Even the movie industry, which definitely is not the primary target of the hacker community is gearing up in anticipation of further cyber-attacks and it is time that we, irrespective of which industry we belong to, gear up too. We need to be alert and be aware that the reason for a breach could either be a highly skilled hacker on the outside or your friendly innocent colleague from the inside!

"Tell me, is something eluding you, sunshine?
Is this not what you expected to see?
If you wanna find out what's behind these cold eyes
You'll just have to claw your way through this disguise"
-Pink Floyd

About Author

Promit Sanyal- *Marketing Manager, Enterprise Security Solutions*

Promit handles global marketing for the Enterprise Security Solutions business in Wipro. He has 7+ years of experience in the IT marketing domain and brings extensive knowledge across product & services marketing spanning product launch, go-to-market strategy, digital & offline marketing campaigns, and last but not the least brand building. In his current role Promit is responsible for enhancing brand value and positioning for Wipro's security business across the globe. Apart from being a music and sports enthusiast, Promit loves reading and learning new languages.