Podcast: SHOW 060 – AN INTERVIEW WITH NEIL DASWANI

This podcast is about the problems with security dealing with Ads and how companies deal with ads on their website to keep them secure. It also talks about Advance Security Certification Program at Stanford and how Google deals with web ad security. They talk to Neil Daswani about web security and the web startup he started.

The podcast creator talks with Neil Daswani, who used to work at Google as a person on their Software Security Group and now is the CTO and co-founder of Dasient which is a web security company. They go on to talk about how Neil had been well involved in security before he ever started Dasient. He had focused on more on webapp security more than regular software security.

Neil talks about how they start with security when they start developing the requirements. He also talks about even though they start developing security into the software from the planning stages, they still have problems and issues in production. Also says there is only so much they can do to prevent attacks, and that they need to have a plan in place to deal with attacks that they cannot prevent. This is in order so they can mitigate the attacks in a timely fashion with as little damage as possible. The podcaster then says that security development in development rarely happens. Neil then says that the defense should be on the appropriate level needed, so with software that needs better security the developers build better security. He then talks about training companies in the practice of security reviews and what the companies can do to better improve software security.

The podcaster then goes on to talk about Google and Dasient and how Google is like a startup. Neil then talks about how he worked in the Security group at Google and how they work with different groups at Google to help secure the different parts of Google software. He talks about that developers need to take into account infrastructure that already exists as much as possible when developing software.

The podcast then changes topics and starts talking about how Dasient is working with securing against malware and other issues in ads on websites. Talks about how malware used to spread via email and links. Now days though the malware is spreading through the web and “drive by downloads” in particular. He explains how drive by downloads use ads or other external networks to download malware to the clients computer with no user interaction. Attackers are using ads more since online
advertising has become very popular and it is spread throughout the internet using ad networks that deliver up ads to the website. It is essentially a distribution network that is already in place for attackers to use to distribute their malware. The attacker creates fake ads that they place on the ad network that are real and then are replaced with malware ads.

The podcaster then brings up the Google blacklist which is used to distinguish resources on the internet that are not safe. This API keeps track of resources that are reported to it by systems and users that are not safe for distribution. When Google works with Ad networks as an example, they are given access to those resources which they then leverage their cloud based scanning system to scan for malicious items. These are then reported back to the resource provider to be taken out of service. Neil says that websites want to find out and mitigate problems before the search companies and sites detect it. They then talk about how it is impossible to secure against all threats and that there is only so much they can do. Also an attacker only needs one exploit. Neil then goes on to talk about how they need to develop technologies to detect and mitigate problems.

Overall this podcast explains a lot about how there are a bunch of ways that security can be an issue on the internet and when developing webapps. It also explains that we need to make sure that we don’t spend all the time trying to prevent attacks and that we spend some time to have a plan in place in case an attack happens and a plan to mitigate it. This helps me in developing secure software by making sure I develop my webapps in such a way that I can keep attacks to a minimum.