**Misuse of Resources**

* **Introduction**
* It is a term for unauthorized access to a system by using its resources (ex. computer within the company network) for malicious purposes.
* **How do these kinds of attacks occur?**
* **Social Engineering**
* This type of attack is where suspects manipulate victims into doing what they want to steal information and use it for malicious purposes.

**Example:**

In 2009, over 20 major software companies such as Google, Adobe, Juniper, and Yahoo fell victim to the **Operation Aurora** targeted attack. In one version of this attack, company employees were lured to the malicious sites via social networking sites and IM clients. Using social engineering techniques the scammers got acquainted with their potential victims, gained their confidence, and did whatever was necessary to make the recipients open a link. Experience shows that to achieve this it was enough to:

1. collect widely available information from social networks about the user, his interests, preferences, and contacts
2. create an account, focusing on the interests of the victim and his personal data (the year and the place of birth, school, college)
3. become “friends” with the people from the victim’s list of contacts
4. get in touch with the victim using an established “cover”

* **Watering Hole**
* The idea of this attack is that a specific group is targeted and then attackers find and infect sites that the members usually visit

**Example:**

In 2013, the site of the U.S. Ministry of Labor was infected but it is assumed that the real target of the attack was the Department of Energy: the criminals were trying to infect the computers of DOE employees who regularly visited the Ministry of Labor’s website.

When a staff member at the company under attack opens the infected site, the code implemented in the body of the page secretly redirects the browser to a malicious site that contains a set of 0-day exploits. Malware posted on infected websites, for example, a server script, often acts selectively to implement malicious code in pages sent to the user who is most relevant to the targeted company. Thus the scammers can hide the targeted attack from antivirus companies and IT security experts.

The fraudsters try to infect trusted legitimate sites. In these cases, even when users must carry out additional steps to run the exploit – to turn on JavaScript, to allow execution of the Java applet to confirm the security exception, etc. – they are likely to innocently click “Allow” and “Confirm”.

A diagram of a diagram

Description automatically generated

**Resources:**

* Katharina.kiener-Manu. (n.d.). *Cybercrime Module 10 Key Issues: Cybercrime that Compromises Privacy*. https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html
* Kruglov, K. (2023, March 27). Security policies: misuse of resources. *Securelist*. https://securelist.com/security-policies-misuse-of-resources/35945/