UNIVERSITEIT TWENTE.

Rijksvastgoedbedrijf
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum
13 december 2019

Referentie
191213MRM9RR01

Opdracht MRM9 - Risk & Resilience Festival 2019

Blogs door S. Boonstoppel & E. van de Ven
About Phishing… & Mission Safety!

About Phishing…

During the Risk & Resilience Festival of 7 November 2019 the 4TU Centre for resilience & engineering was prominently present with multiple speakers. Including a triptych in the afternoon called **’Security and resilience in cyber-physical systems’**.

In this session, as the online preface shows, the speakers discussed some common security treats, together with potential strategies to increase the resilience of these systems, taking into account the most critical system resource, i.e., the human user. It was an interesting and intensive triptych about the increasing influence of cyber on daily business and vice versa. In this blog I want to focus solely on the first subject ‘**Why does the weakest link fail, phishing experiments with humans’ - Pavlo Burda, Phd student @ TU/e**.

The subject starts with an introduction of a whole (criminal) industry based on figuring out how to best exploit the aforementioned human weakness. One of the more well-known practices of cybercrime is phishing. *Phishing* is the deceptive process of obtaining sensitive information by disguising oneself as a reliable source and randomly targeting people, most commonly via email. And more recent via apps and messaging services. *Phishing* is rationale from a criminal perspective. Thirty-two percent of all known cyber breaches involve *phishing* in some way or another. Why do you ask? The answer is simple, it is cheap to operate and easy to repeat. In other words it is a simple cost-benefit equation.

However the practice of *phishing* is becoming more known to the general public and therefor people are slowly becoming more resilient. At the same time cybercrime is constantly evolving. Actions are becoming more and more targeted in order to best exploit weaknesses. When you apply the same base tactic to a specific group of users like employees of a certain company, also called *spear-phishing,* there usually is an underlying goal. This is even more the case when you specifically target high-profile people, also referred to as *whaling*. These newer tactics require more effort in advance, offset by a (possible) high reward. In general the likelihood of a target falling into the trap increases when an attack is more personalized. In hindsight it is not a surprising message, interesting nonetheless.

Applying theory to (semi-)practice, a recent study at TU/e was introduced: **A Spear-phishing campaign targeting the TU/e staff.** First of all and quite possibly the most interesting learning point it is important to mention the sensitivity of the study. As you can imagine it required the necessary preliminary consultations within the university, among others with the ethics board. After much consideration it was agreed that the study could continue under certain conditions, including anonymizing the results on behalf of privacy concerns. In order to make the study al learning experience for the staff of the TU/e, all people who ‘took the bait’ were automatically redirected to a debriefing page.

In short the *spear-phishing* study was about the possibility of influencing the cognitive vulnerabilities, short-cuts in human decision-making. Based on four of the six principles of persuasion as described by Dr. Robert Cialdinii: authority, liking, scarcity and consistency. For example the authority principle is widely used in *phishing*-mails and is based on the tendency of people to obey people in authoritative positions. However is it the most effective method? A second layer was introduced by tweaking the notification method, hence the subject line, personalization & contact information.

Finally some interesting metrics and results of the study which I would like to share.
- The study included 396 subject (all TU/e staff);
- Nine different e-mail groups including a baseline, 44 subjects per research group;
- The phishing-campaign lasted five days in total;
- A total of 90 persons opened the email of whom 61 people submitted their credentials;
- In four hours 75 percent of the victims fell into the trap, incl. seven in the first minute;
- Junior staff are most vulnerable, double the percentage in comparison with the rest;
- Most successful variant, a combination of authority-persuasion & extended contact info;
- In contrast phishing reports are high when using sec authority-persuasion.

Disclosure: our blog about this seminar almost sounds like a recruiting campaign for the criminal industry, it most certainly is not.

Mission Safety!

De Nederlandse krijgsmacht voert bijzondere missies en taken uit in verschillende omstandigheden waar veelal een diversiteit aan risico’s aan verbonden zijn. Om tijdens de uitvoering van deze missies en taken risico’s inzichtelijk te krijgen wordt er risicomanagement toegepast om weloverwogen keuzes te kunnen maken. Het is immers de verantwoordelijkheid van de commandanten om hun personeel zo veilig mogelijk te laten opereren. Dit in achtneming met de bijzondere geweldsmonopolie waar een militair zich in kan of moet bevinden.

Voordat een missie of taak aanvangt wilt een commandant alle reële risico’s inzichtelijk maken. De volgende stap is dan het bewust nemen of niet nemen van mitigerende maatregelen. Door het toepassen van mitigerende maatregelen kan een missie of taak zo veilig mogelijk gemaakt worden. Het is aan de commandant, kijkende naar zijn opdracht of hij het rest risico accepteert of niet. Risicomanagement is een continu verbeterproces. Commandanten moeten hun gemaakte keuzes vanuit het verleden evalueren. Door te evalueren kunnen toekomstige keuzes (beter) gemaakt worden!

Terug naar mission safety! Tijdens de workshop kregen alle deelnemers één missie uitgereikt. Om desbetreffende missie tot een succes te maken moet er risicomanagement toegepast worden. We willen immers dat de missie succesvol is en dat alle militairen veilig thuiskomen! RISKiD heeft een risicomanagement-tool ontwikkeld om ons hierbij te ondersteunen. De tool van RISKiD heeft focus op twee aspecten die veelal als ondergeschikt belang worden gezien: samenwerking en gebruikers gemak. In de tool worden meerdere stappen, gezamenlijk online of offline doorlopen. Tijdens desbetreffende stappen worden risico’s geïdentificeerd, beoordeeld en besproken. Daarnaast worden beheersmaatregelen bepaald en helpt de tool risico-eigenaren gemaakte keuzes te monitoren. Ten einde zijn alle uitkomsten duidelijk te overzien in een dashboard, dit stelt de risico-eigenaren in staat om alle risico’s (en genomen mitigerende maatregelen) overzichtelijk, transparant en up to date te houden!

Met de tool van RISKiD kan risicomanagement samen, simpel en snel toegepast worden in de dagelijkse praktijk. Dit was terug te zien tijdens de workshop, alle deelnemers hadden al snel feeling met het gebruik van de risicomanagement-tool.

Samenvattend, een tool zoals RISKiD kan commandanten (en risicomanagers) op weg helpen naar het bereiken van mission safety!