Contribution ID: **18** Type: **Presentation (25 minutes)**

Resilience in Action: Lessons from SURF's Red Team Testing Initiatives

Wednesday, 10 April 2024 13:30 (20 minutes)

In the realm of cybersecurity, the true test of any protective measure lies in its real-world performance. While institutions have to cover a broad range of possible attack vectors, an attacker only needs a few holes to attain their goals. At SURF, we are exploring how we can help the sector with red teaming and other types of resilience tests to asses their IT landscape from a hacker's perspective. This presentation will explore SURF's initiatives around cyber resilience testing, sharing our approach to the broader theme of assessment, testing an practicing. It will cover three areas: what role testing can take in a broader cyber resilience strategy, SURF's specific initiatives in this field in developing (knowledge) products and services, and real-life technical findings from our red teaming tests.

Within SURF, we have an innovation zone for cybersecurity. The different areas of this program emphasize the multifaceted needs to get security maturity in the sector to a higher level. Besides the technical services we deliver, we work on (frameworks for) audit and compliance, risk management, awareness, knowledge sharing, crisis management and connections to other types of security. It shows how complex cybersecurity is: at the core you have to take measures to protect the CIA (confidentiality, integrity, availability) of information, but in order to do that effectively you have to make risk trade-offs, figure out workable procedures, audit your procedures and policy and make sure your students and staff actually adhere to the policy. To us, testing your defense, detection and response to an actual cyber threat is the icing on the cake of a holistic approach towards cybersecurity, and may be the only way to know if what you did was any good.
In the past year, we explored the theme of cyber resilience testing broadly. Talking to organizations with a similar position in the Netherlands (the healthcare CSIRT, association of municipalities, national government, etc.) we discovered that many of them are taking initiatives in this area, and that we can already help our members by simply sharing their insights within SURF. This led to the development of documents that guide the different steps of resilience tests: choosing the type of test most suitable to your goals, procuring the test, make arrangements with a provider, the many things you can do to get the most out of your test, and how to share outcomes. Besides advice, SURF got involved by taking part in the white team (observation/steering) of several test. We discovered that this is incredibly valuable, both to the organization who can benefit from extra experience and knowledge, as well as to us. We can extract many, many learnings from these experiences and help the next organization to be better prepared for their exercise. Oh, and it's a lot of fun to be one of only six people who know how deep hackers currently are in the network of a large university.
In this presentation, attendees will gain insights into the essential role of assessment, testing, and practicing as part of an approach to cyber resilience. The target audience is both those who are involved with cyber resilience at the strategic level, as those who just want to know what mistakes other institutions made so they don't have to make the same ones. We will share SURF's initiatives in this domain, offering practical examples that can inspire and guide others in supporting their cybersecurity efforts. Furthermore, we'll discuss specific learnings from our red teaming tests, shedding light on how these insights impact the rest of the sector's cybersecurity and network operations. Other NREN's can learn from our experiences and adapt these to their contexts.

Primary author: GADELLAA, Joost

Presenter: GADELLAA, Joost

Session Classification: Security Products

Track Classification: Presentation