Why a Red Team Exercise Delivers Results: *A case study looking at a recent Red Team Engagement.*

Technology has changed the way businesses fundamentally operate and work in an interconnected world which has enabled organisations to be more productive, efficient and provide a wider range of services. Whilst overall this is a good thing, it has created a significant number of threats and increased risks to organisations most prized assets: information and knowledge.

The potential consequences of a data attack or 'hack' should have CISOs and CIOs panicking. Part of having a solid information security program is to build in periodic testing. One of the most efficient ways to test your environment is to simulate *a real-world attack* or as Dionach and other cyber security testing companies would call, a Red Team Attack.

Benefits of a Red Team Assessment

Unlike traditional penetration testing or social engineering, Red Team Attacks are designed to simulate the likely root causes of a cyber-attack. This may include but not limited to technology, staff and physical locations, all with the goal of extracting information and assets. Additionally, Red Team Attacks should actively test your defences (Blue Team) to ensure that any unauthorised activity is immediately identified and investigated accordingly.

Results of Conducting a Red Team Assessment:

- Understand whether the most critical asset in your organisation is at risk
- Test the detection and response capabilities of your Blue Team, SIEMs, SOCs
- Uncover serious security flaws that would not otherwise be detected with traditional penetration tests
- Provide an evidence-based risk profile to board of directors and senior-level management or stakeholders

- Gauge the potential cost of a breach to the organisation versus the cost for an attacker to execute a successful attack
- Assist with quantifying the return on investment (ROI) in cyber and information security

The Process

A Red Team assessment follows a stealthy dynamic attack path and attempts to achieve the pre-defined goals through the following phases:

Your Report

When the Red Team Assessment is complete, Dionach will provide a report that includes:

- Executive summary for senior-level management
- Attack path scenarios for post-breach analysis
- Technical recommendation for fixing discovered vulnerabilities
- Strategic recommendations for long-term improvement

Along with your report, Dionach will present the results in a post-assessment briefing which gives the opportunity to discuss the findings and provided recommendations.

Dionach can also assist the SOC or Blue Team with the following tasks:

- Review of the audit logs and alerts to check if there are any trace of the activity performed by Dionach Red Team
- Assist your SOC or Blue Team to configure alerts in order to detect these attacks
- Test the newly configured alerts by re-running the attack scenarios of the RT assessment

Real World Example

Context

A large multinational fintech engaged Dionach to conduct a Red Team assessment in order to evaluate their ability to detect and respond to real world cyber security attack.

The company had a mature security program including the following:

- An established Information Security Management System (ISMS) and Information Security Governance program
- Good technical security controls protecting the network perimeter including and cloud environment including next generation firewalls, SIEM (Security Information and Event Management), and endpoint security solutions
- Outsourced (SOC) Security Operation Centre
- Highly motivated and skilled blue team ready to react when an alert is triggered
- Automated password audit systems which notified account holders via email if they have chosen a weak password
- Regular social engineering tests and security trainings to raise awareness among staff
- Regular external and internal penetration tests

The assessment had two objectives:

- Gaining access to a small number of servers containing mission critical data.
- Assessing the capabilities of the blue team including how quickly they detect and respond to a cyber security attack.

Reconnaissance

As with all Red Team Assessments the team started by collecting as much information as possible about the target using publicly available open-source intelligent resources and by reviewing the company's exposed attack surface. These included, but were not limited to, the following information:

- Staff details
- Physical office locations
- Publicly exposed systems, applications and services
- Remote access solutions
- Mobile applications available on the app store
- Social media profiles

Initial Plan

During the initial reconnaissance phase, it was discovered that staff were required to use multi-factor authentication to access their emails using desktop application Outlook or a web browser to

access Office365. However, upon further inspection Dionach discovered that a second factor was not required when access to emails was done via Outlook mobile app.

With this knowledge, Dionach's Red Team decided to use a phishing campaign to target a select number of employees in order to obtain valid login credentials.

Phishing Campaign

The team sent a phishing email which persuaded the victim to login to a fake portal hosted on a Dionach server in order to obtain valid credentials.

While a small number of users clicked on the malicious link sent in the email, none of them submitted their credentials. This could be attributed to the regular social engineering tests and security awareness training delivered to staff.

A New Angle

After the failed phishing campaign, the team went back to the drawing board to come up with a new plan of attack.

Reviewing the company's Twitter account, the team discovered that they host a monthly community event at one of their buildings. The team registered for the event with the aim of deploying a purpose-built device into their internal network. The device will allow the team to gain remote access to the network using either an independent wireless connection or 3G/4G mobile connection.

The Event

Two members of Dionach's red team attended the event. Once they familiarised themselves with the environment. The team managed to slip away from the main event to see if there were any unlocked offices or conference rooms. Once a room had been found. One team member acted as a lookout while the other plugged the device and checked that he could reach it from his mobile phone. Shortly afterwards the testers left the event and joined the rest of the team in a coffee shop down the road.

Internal Network Access

Once connected to the network, the team started mapping the internal network and gathering additional information. Over the next couple of days, the team captured several password hashes, which was achieved by exploiting a weakness in Windows' broadcast protocols. However, users appeared to be using strong complex passwords and it was not possible to crack the hashes to recover clear-text passwords. The team then decided to relay a captured hash belonging to a user and use it to login into a workstation where they had local administrative privileges. This allowed them to extract the clear-text password of the currently logged in users from memory.

Phishing Emails from a Trusted Source

Do you remember the Outlook mobile app's lack of multifactor authentication? This flaw combined with the obtained credentials permitted Dionach's Red Team to access corporate emails remotely,

without raising any security alert. Although traditional penetration tests were regularly performed by the organisation, such security flaw remained uncovered.

With an access to emails, the team extracted the following information:

- Software installed
- Internal web applications
- Suppliers
- Client names
- On-going projects
- Meetings planned in the Calendar

After the information gathering period, Dionach used the obtained information to target a highly privileged user with a phishing email through one of the compromised email accounts. As the email came from a trusted source and utilised a pre-existing conversation chain, the target executed the payload in the email and granted Dionach remote access to their machine.

Privileged Internal Network Access

Once privileged administrative level access was obtained, the team was able to easily maintain persistence and move laterally across the network in order to gain access to the targets agreed with the client.

Key Takeaways

Following the engagement Dionach conducted a workshop with the blue team to ensure the transfer of knowledge and help them improve:

1) Most of the users who received our initial phishing email did not report it. One user did report the email and raised a support ticket. However, since they were not one of the employees who clicked on the link, they were simply advised to delete the email.

2) The blue team did not properly investigate the reported phishing email by checking if other staff members received the same email and if any of them have clicked on the link or submitted their credentials.

3) While physical security was appropriately enforced on the entry points to the building. Once inside physical access control was not enforced on all doors such as meeting rooms.

4) Physical security was not properly enforced during events to ensure that attendees do not wander into places they are not authorised to access.

5) The purpose-built device was not discovered. The team retrieved it during the blue team workshop.

6) Network access control was not enforced, and the team were able to connect unauthorised devices to the local network.

7) Some of the actions performed by the red team were picked up by some of the monitoring devices. However, the SOC did not follow standard operating procedures and investigate the reported security events. Understandably, this resulted in some serious discussions between our customer and their SOC provider.

8) Finally, while some of our actions were picked up by some of the alerting and monitoring systems, a large number were not picked up. Dionach worked with the client to help fine tune their monitoring devices to ensure that similar attacks will be detected in the future. Dionach then reran some of the attack scenarios to ensure that the actions performed by the team were detected and the relevant systems and personnel were alerted.

More Red Team Examples

In another Red Team assessment, Dionach Red Team reverse engineer one of the customer's mobile apps available on Apple Store and Play store in order to gain a foothold on the internal network. The assessment is discussed in technical detail in our blog posts "A Brief Story of a Red Team Security Assessment" Part1 and Part2 which describe the whole attack path. Additionally, Dionach gave a talk at DefCamp 2019 that explored this matter further. The conference video for this talk can be seen below:

https://www.youtube.com/watch?v=Hx9EBQT4BBc

Contact Dionach

Dionach is an independent CREST-approved global provider of information security solutions. With a twenty-year track record of delivering insight-led cybersecurity services to organizations worldwide, we are the ideal partner to strengthen your cyber resilience, mitigate risk and safeguard your most valuable information assets right across the enterprise.

We are proud to be ISO 27001-certified, a PCI Qualified Security Assessor (QSA) and one of just 22 companies worldwide to hold the status of PCI Forensic Investigator (PFI). This testifies to the industry-leading competence of our technical specialists and our dedication to achieving the highest possible standards in service delivery.

Over 200 public and private sector organizations worldwide currently entrust their cyber security to our expanding global team.

For more information on Dionach and how we can assist your organization, please contact us via www.dionach.com or call and speak to one of our consultant representatives.