www.pwc.pl/bezpieczenstwo-biznesu

PwC STRIKE

(Short-Term Real Intrusion and Hacking Exercise)

Unauthorized access to sensitive resources is usually possible within

4 hours

We would like to offer a security assessment that tests the first line of defense against **intrusion into systems and sensitive information** of your organization.

During a few hours spent in your company we will determine what possibility of accessing the resources has a person without any explicit privileges granted.

Using a set of techniques including technology-based and social engineering, we will attempt to access sensitive information within limited time of about **6 hours**.

Our tests will be a combination of the two scenarios described in more detail on the following page:

- a meeting in the conference room,
- a guest at the reception desk of the company.

If the security measures are found not to be satisfactory, we can help you with possible next steps.

70%

of attacks are caused by disgruntled employees

4%

of firms lost more than PLN 1m due to security incidents

33%

of reported security breaches resulted in financial loss

5%

of firms reported a downtime in business for 5 days

Source: Pwc Report „State of Information Security in Poland 2016”

pwc

PwC STRIKE

We propose an analysis based on elements of the two previously mentioned scenarios. The scope of work will be specifically tailored to the characteristics and environment of your organization. The work will also be preceded by a meeting at which you will be able to express your needs and preferences. Below we present assumptions that we have made so that the analysis gives you reliable results.

We will attempt to:

- obtain access to restricted zones and facilities,
- unlock password-protected corporate computers,
- obtain access to a wireless or wired corporate network,
- identify key business systems,
- analyze security of identified systems,
- obtain access cards and make clone copies,
- move from guest network to your office network or to server network,
- attract employees to specially crafted web pages or connect specially prepared device to their computers.

We assume:

- that we start with:
  - own laptops,
  - access to conference room,
  - access to guest network,
- and we do not have:
  - access to your corporate computer,
  - corporate login names or passwords,
  - keys or access control cards,
  - information about network structure,
  - information about location and architecture of business systems.

We will not:

- destroy elements of physical security or data sets,
- cause danger to personnel or security officers.

We would like to ask you:

- to assign a coordinator who will be aware of the assessment in case of intervention of personnel or security officers,
- refrain from actions that go beyond the usual daily habits (e.g., temporary hardening protection measures or informing staff about the analysis performed, etc.).

Contact

Rafał Jaczyński
Director, Security & Revenue Assurance Practice Leader
+48 519 507 122
rafal.jaczynski@pl.pwc.com

Patryk Gęborys
Vice-director, Cyber Security Team
+48 519 506 760
patryk.geborys@pl.pwc.com