Social Engineering Assessment

Our Social Engineering Assessments test how easy employees are to manipulate, and they take a variety of forms – from USB-stick ‘drops’ to sophisticated phishing emails. We will try to be as smart as a hacker or cyber criminal will be, even posing as technicians or systems administrators to fool employees.

Cognosec Services

Features

Assessment of your social engineering risks can be an add-on to penetration testing or a separate initiative to increase employee awareness. Either way, it should be a serious consideration for any organisation. Lack of awareness among employees can potentially be more dangerous for an organisation than outdated systems. While breaking into an IT system might take weeks or months, a simple call takes just a few minutes, an email even less. Beside than the fact that Information Systems are becoming increasingly complex, one of the key reasons that Social Engineering is so heavily utilized is its low cost to benefit ratio. It can be much faster to simply pick up a phone, pretend to be someone else and ask for a password than it would be to scour source code for any small weakness in IT systems. Targeted individuals do not usually suspect that they are or could be a victim of social engineering, yet the impact of divulging even small, seemingly meaningless pieces of information can be disastrous. This data can be accumulated and used to assume identities of employees and fish for even more valuable information by phone and email, gain

access to buildings and restricted areas, plant rogue network devices and continuously monitor data traffic.

Description

Social engineering, in the context of information security, refers to manipulating people into divulging confidential information – or performing acts that put an organisation's data assets at risk. It differs from a traditional 'con' in that it is often one of many steps in a more complex fraud scheme, but, like a traditional con, it exploits human curiosity and gullibility and the natural desire to please or co-operate with others. Our Social Engineering Assessments test how easy employees are to manipulate, and they take a variety of forms – from USB-stick 'drops' to sophisticated phishing emails. We will try to be as smart as a hacker or cyber criminal will be, even posing as technicians or systems administrators to fool employees. The assessments have an important role to play in raising awareness – and can help convert employees from potential victims into first responders who spot and report attempted attacks.

Specifications

Cognosec's Social Engineering is a vital element of a complete penetration test. Once the scope of the testing and accompanying success criteria's have been determined, our experts will perform any number of social engineering tactics to try and gain access to defined in-scope systems. Cognosec will only perform these tests in areas that have been agreed upon contractually. Any in-scope data extracted or handled during the process will be securely deleted.

Sweden
Cognosec Nordic AB
Birger Jarlsgatan 12
114 34 Stockholm
Sweden
Tel +46 (0)8 400 170 00
sales.se@cognosec.com

UK & Ireland
Cognosec Limited
3rd Floor
The News Building
3 London Bridge Street
London SE1 9SG
UK
Tel +44 (0)20 3870 1539
sales.uk@cognosec.com

Germany
Cognosec GmbH
An der Welle 4
60322 Frankfurt
Germany
Tel +49 (0)69 7593 8490
sales.de@cognosec.com

Austria
Cognosec GmbH
Castellezgasse 16/2
1020 Vienna
Austria
Tel +43 (0)1 212 2020
sales.at@cognosec.com

UAE
Cognosec DMCC
2202 Indigo Icon Tower
Cluster F
Jumeirah Lakes Towers, Dubai
UAE
Tel +971 (0)4 451 1552
sales.dxb@cognosec.com