| | | |
|---|---|---|
| 1. | Record Nr. | UNINA9910138859303321 |
| | Autore | Assing Dominique |
| | Titolo | Mobile access safety [[electronic resource] ] : beyond BYOD / / Dominique Assing, Stephane Cale |
| | Pubbl/distr/stampa | Hoboken, N.J., : ISTE Ltd./John Wiley and Sons Inc., 2013 |
| | ISBN | 1-118-57788-4 |
| | | 1-118-57798-1 |
| | | 1-118-57781-7 |
| | | 1-299-18667-X |
| | Descrizione fisica | 1 online resource (248 p.) |
| | Collana | Networks and telecommunications series |
| | Altri autori (Persone) | CaleStephane |
| | Disciplina | 005.8 |
| | | 621.384 |
| | Soggetti | Computer networks - Remote access |
| | | Computer networks - Security measures |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Note generali | Description based upon print version of record. |
| | Nota di bibliografia | Includes bibliographical references and index. |
| | Nota di contenuto | Title Page; Contents; Introduction; Chapter1. An Ordinary Day in the Life of Mr. Rowley, or the Dangers of Virtualization and Mobility; 1.1. A busy day; 1.2. The ups and downs of the day; 1.3. What actually happened?; Chapter 2. Threats and Attacks; 2.1. Reconnaissance phase; 2.1.1. Passive mode information gathering techniques; 2.1.2. Active mode information gathering techniques; 2.2. Identity/authentication attack; 2.2.1. ARP spoofing; 2.2.2. IP spoofing; 2.2.3. Connection hijacking; 2.2.4. Man in the middle; 2.2.5. DNS spoofing; 2.2.6. Replay attack; 2.2.7. Rebound intrusion |
| | | 2.2.8. Password hacking2.2.9. The insecurity of SSL/TLS; 2.3. Confidentiality attack; 2.3.1. Espionage software; 2.3.2. Trojans; 2.3.3. Sniffing; 2.3.4. Cracking encrypted data; 2.4. Availability attack; 2.4.1. ICMP Flood; 2.4.2. SYN Flood; 2.4.3. Smurfing; 2.4.4. Log Flood; 2.4.5. Worms; 2.5. Attack on software integrity; 2.6. BYOD: mixed-genre threats and attacks; 2.7. Interception of GSM/GPRS/EDGE communications; Chapter 3. Technological Countermeasures; 3.1. Prevention; 3.1.1. Protection of mobile equipment; 3.1.2. Data protection; 3.2. Detection; 3.2.1. Systems of intrusion detection |

| | |
|---|---|
| Sommario/riassunto | Over recent years, the amount of mobile equipment that needs to be connected to corporate networks remotely (smartphones, laptops, etc.) has increased rapidly. Innovative development perspectives and new tendencies such as BYOD (bring your own device) are exposing business information systems more than ever to various compromising threats. The safety control of remote access has become a strategic issue for all companies. This book reviews all the threats weighing on these remote access points, as well as the existing standards and specific countermeasures to protect companies, from both th |