REDNER

NAME
Benedikt Strobl

KONTAKT
NSIDE ATTACK LOGIC GmbH
Agnes Pockels-Bogen 1
D-80992 München

BIOGRAFIE

Benedikt Strobl
IT Security Analyst

Herr Strobl arbeitet seit 2015 in der IT-Security und war zuvor seit 2011 als Entwickler tätig. Als Penetrationstester war er an diversen Red Team Assessments beteiligt, simulierte zahlreiche Phishing-Angriffe und leitete eine Vielzahl an externen wie internen Penetrationstests auf Systeme, interne Netzwerke und Active Directorys bei vielen namhaften Unternehmen. Darunter führende Unternehmen in der Kommunikations-, Versicherungs- und Finanzbranche, sowie große Industrieunternehmen.

Seine technischen Spezialgebiete umfassen unter anderem:

- Phishing Simulationen und Social Engineering
- Web Application Hacking
- Windows Host und Active Directory Security
- Linux Host Security

VORTRAG

Live Hacking

Fast alle Fälle gezielter Betriebsspionage und IT-gestützter Angriffe auf Unternehmen nutzen die Schwachstelle Mensch als Einstiegspunkt. Dadurch werden nicht nur Informationen abgegriffen, sondern meistens direkt Schadsoftware auf einen Rechner im internen Netz geschleust. Dieser Weg wird nicht ohne Grund gewählt: Es ist oft der einfachste Weg. Deshalb ist ein wichtiger Schritt für die Verbesserung der Sicherheit, die eigenen Benutzer zu informieren und so auf Angriffe vorzubereiten.

Viele Menschen glauben nur das, was sie mit eigenen Augen gesehen haben. Deshalb wird demonstriert, wie professionelle Angriffe auf IT-Systeme durchgeführt werden. Es wird über tatsächliche Vorkommnisse und eigene Erfahrungen aus der täglichen Arbeit berichtet.

Durch diese Awareness-Vorführung bekommen die Teilnehmer die Möglichkeit hinter die Kulissen von Hacker-Angriffen zu blicken. Es wird gezeigt, wie Hacker und Spione wirklich ticken. Welche Tools und Tricks sie verwenden. Wie man ihre heimlichen Attacken frühzeitig erkennt und sich am besten vor ihnen schützen kann.

Ganz nach dem Motto „Kenne deinen Feind!“ schafft dieser Vortrag ein hohes Bewusstsein und damit einen der besten Schutzmechanismen, die „User Awareness“.

Folgende Thematiken können im Live-Hacking genauer beleuchtet und demonstriert werden:

- Vorgehen eines modernen Red Teams
- Open Source INTelligence (OSINT)
- Gezielte Malware-Angriffe
- Social Engineering
- Mobile Security
- IoT- und Roboter-Hacking