Blue Frost Security

EINLADUNG

27.09.2017

Grandhotel Hessischer Hof
Friedrich-Ebert-Anlage 40
60325 Frankfurt am Main

SCHWACHSTELLEN IN KRITISCHEN INFRASTRUKTUREN

AGENDA

08:30 REGISTRIERUNG MIT KAFFEE & GEBÄCK

09:00 BEGRÜSSUNG

09:15 FROM THE SMALLEST CHIP TO THE BIGGEST DATABASE – PASSWORDS ARE YOUR FIRST AND LAST LINE OF DEFENCE

einziger Vortrag auf Englisch!

No matter what any commercial vendor says, passwords are still the most common way of securing access to systems & data everywhere. Regulatory requirements such as GDPR & PSD2, as well as standards bodies such as NIST, ISO & PCI, continue to evolve and set more pressure on how to secure your customer data. Do you think you are secure?
Per Thorsheim, security advisor & password security expert

09:45 WE MAKE YOUR VULNERABILITIES GREAT AGAIN – EIN BLICK AUF DAS TÄGLICHE SPIEL MIT DEN SCHWACHSTELLEN

Täglich werden neue Schwachstellen gemeldet, aber können Sie einschätzen, wie viele und welche Produkte am häufigsten betroffen sind?
Wir geben Ihnen einen Einblick in den Lebenszyklus bekannter Schwachstellen, angefangen bei ihrer Meldung, bis hin zum Roll-Out des Updates und den potenziellen Auswirkungen auf Ihr Unternehmen.
Benjamin Gnahm, Senior Security Researcher

10:15 BROWSER SICHERHEIT UND ZERO DAY EXPLOITS – WIE SICH KRIMINELLE ZUGRIFF AUF IHR NETZWERK VERSCHAFFEN

Berichte aus dem BFS Labs Forschungslabor über die Methoden, mit denen Schwachstellen in den verbreitetsten Softwareprodukten wie Windows oder Browsern entdeckt werden und wie solche Schwachstellen bereits aktiv bei Angriffen auf Banken und andere kritische IT-Infrastrukturen ausgenutzt wurden. Demonstration eines Exploits auf den Internet Explorer 11.
Moritz Jodeit, Director of Research

10:45 KAFFEEPAUSE

11:00 CASE STUDY – SICHERHEITSRISIKO: SECURITY APPLIANCES

Die meisten Sicherheitsverantwortlichen fühlen sich mit einer zusätzlichen Sicherheitsappliance sicherer. Unternehmen verwenden üppige Budgets für die Anschaffung dieser Lösungen. In den meisten Fällen erhöhen sie damit jedoch ihre Angriffsfläche deutlich.

Welche Risiken bestehen bei der Installation einer Security Software oder Hardware in Ihrem Netzwerk?

Unsere Case Study zeigt eine Schwachstelle, die wir während eines routinemäßigen Penetrationstests in einer FireEye Appliance gefunden haben und deren Ausnutzung Vollzugang zum Netzwerk des Kunden ermöglicht hat.

Beispiele ähnlicher Findings in diversen Security Produkten. *Dr. Jan Sima, Senior Security Analyst*

11:30 PENETRATIONSTEST VON PROPRIETÄREN PROTOKOLLEN AN EINEM BEISPIEL AUS DER FINANZWELT

Branchen entwickeln in vielen Fällen eigene Systeme und Protokolle, die von den Unternehmen aus dieser Branche eingeführt und verwendet werden. Da diese Systeme und Protokolle keinem Standard entsprechen, tun sich viele PenTester schwer damit, diese zu testen, schließlich gibt es keine öffentlich verfügbaren Test-Tools.

Wir zeigen anhand eines Beispiels aus der Finanzwelt wie wir proprietäre Protokolle analysieren, eigene Tools für derartige Tests entwickeln und so effektiv proprietäre Protokolle testen.
Moritz Jodeit, Director of Research

12:00 ZUSAMMENFASSUNG & DISKUSSION

12:15 GEMEINSAMES MITTAGESSEN UND NETWORKING