BLK: Account-Hygiene – Mehr als Händewaschen,
Schutz gegen Credential Theft Angriffe

Datum: **Do, 22.09.2016 – 16:00 Uhr – 16:30 Uhr , HS 0.18**

Referenten: **Torsten Witte, Informationssicherheits-Manager, Zentraler IT-Betrieb Niedersächsische Justiz**

Thorsten Bruns, Dipl. Rechtspfleger, Niedersächsisches Justizministerium

Protokoll: **Dominique Bosle**

Die Referenten machten eingangs klar, dass sich die Angreifer innerhalb der Mauern befänden, die Informationstechnik-Landschaft also keine herkömmliche Burg mehr darstelle, da deren Mauern verwischt seien.

Die Cybersecurity stünde demnach vor der Herausforderung, auf die heutige, über 4 Wände hinausgehende Infrastruktur zu reagieren, was bei der wachsenden Flexibilität (z.B. Nutzung mobiler Endgeräte) recht schwierig werde.

Wichtiger Ansatzpunkt sei die Sensibilisierung der Menschen, denn die Angriffe könnten bereits bei *einem* falschen Klick eines Einzelnen innerhalb einer noch so gewissenhaft und vorsichtig agierenden Gruppe erfolgen.
Oft wirkten Schutzmaßnahmen aufgrund der Komplexität nur noch im Nachgang an eine bereits erfolgte Attacke.

So könne man sich beispielsweise im Cybernet einkaufen, ohne selbst tätig zu werden, was eine 100%ige Sicherheit undenkbar macht.

Die Referenten unterschieden in einem Schaubild zwischen 2 Abgriffmöglichkeiten in Windowssystemen, dem 'Pass-the-Hash' (entdeckt 1997) und dem 'Pass-the-Ticket' (entdeckt 2010).

Dargestellt wurde der zeitliche Ablauf eines Angriffs. Eine Schad-Mail erreicht den PC, das Schadprogramm gelangt auf den PC, eine Kennwortauslesung erfolgt binnen 24-48 Stunden / Schnitt. Allerdings erfolgt die Entdeckung eines Angriffs erst in 11-14 Monaten / Schnitt, was dem Täter eine Menge Zeit einräumt.
Dies belege u.a. ein Angriff auf den Deutschen Bundestag, der 3 Jahre lang unentdeckt blieb.

Tückisch seien Emails, die vermeintlich vom ortsansässigen Schützenverein oder einem Schulfreund stammen und somit den Empfänger veranlassten, wie selbstverständlich diese zu öffnen. Professionelle Täter unterlägen auch nicht der Gefahr, durch ein 'Denglisch' an ihrem Plan zu scheitern.

Insbesondere, weil bereits ein einzelner Nutzer zum Zerschießen einer ganzen Infrastruktur beitragen könne, müssten Überlegungen angestellt werden, wie dieser Situation zu begegnen sei. Die Idee nun lautet, die Infrastruktur in ihren Ebenen zu schützen und so zur Schadensbegrenzung in verschiedenen Sicherheitsschichten beizutragen.

Als Präventivmaßnahmen wurden aufgeführt:

1. Admin Workstations und Logon Restrictions
2. Zufällige lokale Admin-Passwörter
3. RDP / Restricted Admin Mode

Das Vorgehen gliedert sich in eine IST-Analyse (Was gilt es zu schützen?), Schutzmaßnahmenfindung, Zuordnung der Schutzmaßnahmen zu administrativen Ressourcen, Maßnahmenumsetzung (LAPS u.Ä.), Projektbegleitende Admin-Schulungen und PEN-Tests (Haben die Maßnahmen gegriffen?).

Die Hürden lägen in der Zuordnung der administrativen Ressourcen zu den Sicherheitsschichten ('Tiers'), der Veränderung der bestehenden Workflows, der teilweise geringfügigen Verlängerung des Anmeldeprozesses für Admins, der Trennung bestehender Admin-Konten für mehrere Sicherheitsschichten, etc .

Als Lösungsansatz wurde sodann als Fertigpaket sicherer Administration das ESAE (Enhanced Security Admin Environment) vorgestellt:

Ohne ESAE beliefen sich das Personal auf 50 PT extern und 100 PT intern, die Haushaltsmittel auf 125.000 €, mit ESAE beliefen sich das Personal auf 300 PT extern und 200 PT intern, die Haushaltsmittel auf 750.000 € bis zu 1 Million Euro.

Im Anschluss stellte ein Teilnehmer aus dem Publikum die Frage, ob man nicht früher auf Angriffe reagieren sollte durch Vorsorgemaßnahmen. Die Referenten verwiesen beispielsweise auf die Existenz intelligenter Firewalls.