How to Hack your Client and…his Service Provider(s)

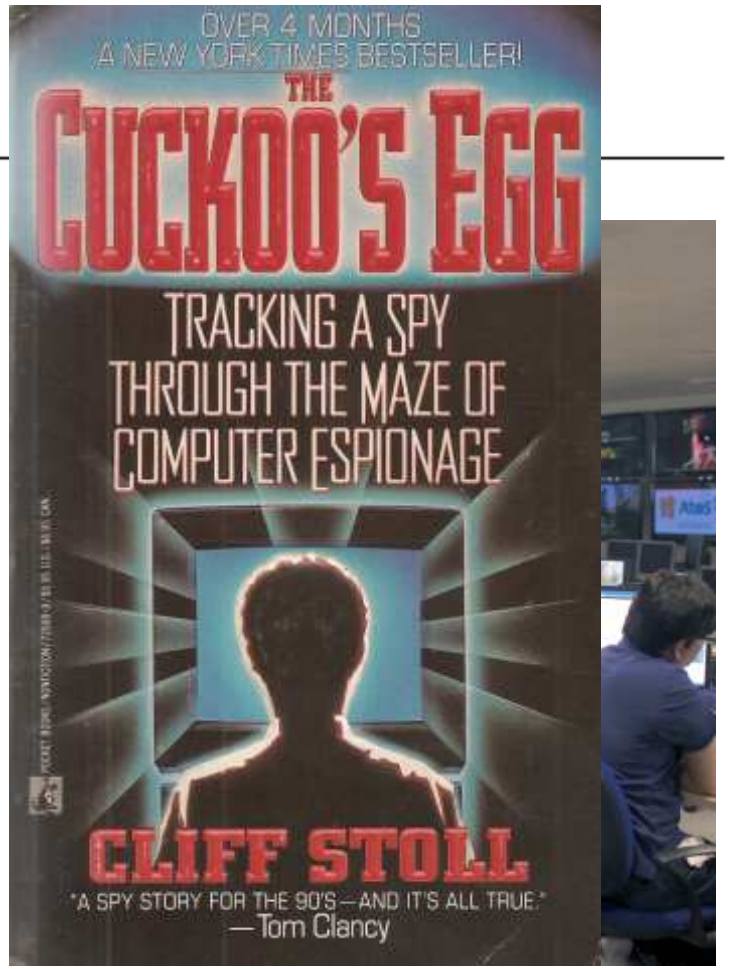
Paul W.M. Oor CISSP, CISM, CIPP/E
Chief Security Officer

ISACA Roundtable, Breukelen (NL)

2 March 2015

Atos

Once upon a Day…



6 November

- Unexplainable Login Attempts
- Traced to a VM Mac Address
- Disappears

4 December

- Similar Connection Attempts
- Extra Logging on Switches

6 December

- Port Monitoring in Place
- ~10 Minute Scans, Login Attempts…
- IP Addresses related to the Mac Address now Identified
- VM disappears again…

Once upon a Day

11 December

- (Customer) Location Identified

12 December

- Team on Location…
- Trace Route, Switch Monitoring,
- Accessing the Patch Panel
- Network Outlet and…
- Room Identified !!

Disclaimer

"The Opinions expressed in this Presentation are those of the Speaker and do not necessarily reflect those of past or present Employers, Partners or Customers."

The Traditional Case…

Traditional Governance…

- ▶Responsible
- ▶Accountable
- ▶Consult
- ▶Inform

Todays Case…

Governance…

- Responsible
- Accountable
- Consult
- Inform

Constraints…

"If access isn't authorized there's an offence under national and international laws. Prosecution might be the result."

"The authorized access offence covers everything from guessing the passwords to accessing someone's webmail account, cracking the security of a bank etc.

Unauthorized access even to expose vulnerabilities for the benefit of many is by default not legal, even when executed following 'responsible disclosure guidelines'."

Modus Operandi

How to facilitate this anyway...?

1. "Ethical Hacking (security tests): Procedures and Guidelines for Security Stress Tests"
2. Security Assessment & Non Disclosure Agreement (SA&NDA)

The primary Objective of Ethical Hacks and Penetration Tests is to improve Security.

Modus Operandi

Minimize Business (Continuity) Risks

Maximize Effectiveness

Assessment methods…
- Examination
- Testing

Types of tests
- Limited
- "Creative"
- and… anything in-between…

Procedure and guidelines
- All Approvals (RACI)
- Standardization SA&NDA / Test Plan
- (Minimum) Requirements
- Awareness and Acceptance by ALL
- Prevent Business Continuity Issues

Legal stuff…

(All) parties involved

- 2-way NDA or
- 3-way NDA or…

Address:

- Purpose
- (Non)-Disclosure, Confidentiality, IPR
- Staff involved
- Communication, Notifications
- Indemnification
- Scope: “Do-not-cross-this Line!”
- Fines, Fees and other Costs
- Second Opinion
- Termination
- Jurisdiction
- Reporting

Test Plan (Limited Test)

- Policies, Professional References
- Test Window (retest?)
- Scenario Description
- Communication with Operations
- "Emergency Stop' Procedure
- Logging
- Risk Register
- Safeguard Personal Data
- 'Logistics'
- Originating IP Addresses
- Description of the Tools
- Test Universe
- Clean-Up Arrangements
- Test Results

Test Plan (Creative Test)

ADD-ON's

- In-depth..
- Liaisons/Chaperones/Sentries
- Monitoring

- Policies, Professional References
- Test Window (retest?)
- Scenario Description
- Communication with Operations
- "Emergency Stop' Procedure
- Logging
- Risk Register
- Safeguard Personal Data
- 'Logistics'
- Originating IP Addresses
- Description of the Tools
- Test Universe
- Clean-Up Arrangements
- Test Results

Reporting…

AND…

Risk Description and/or Assessment

Always

- Distribution, Audience
- Vulnerabilities
- Mitigation Advise
- Preview/Comments Security

Recommended

- Business Management Summary
- Recommendations
- Statement of Confirmation
- Description of
  - Terminology
  - Context
  - Scenario’s
  - Risk Evaluation Criteria

Complicated?

Remember…

Our Primary Objective of Ethical Hacks and Penetration tests is to improve Security

Not to enable, underpin or otherwise generate Legal and Financial claims…!

Take away's…

1. Verify Credentials, Certification and Track Record of the Ethical Hacker and his Employer
2. Ensure compliance with (any) standard or best practices, e.g. OWASP, PTES etc.
3. Test Plan: Rules of Engagement!
4. Issuing a Get-Out-of-Jail Card should be a serious topic for Business Managers
5. A 'responsible disclosure statement' isn't the same thing…
6. You DO (!) want to review the Final Draft of the Report
7. Consider a 'subscription' approach and agreements

QUESTIONS?

Thanks

For more information please contact:
M+ 31 6 539 74 512
paulwmoor@gmail.com
paul.oor@atos.net

Dit bericht sturen wij ter informatie.

Geachte Paul,

In verband met ziekte komt de presentatie van dhr. Delpeut voor de Round Table van maandag 2 maart te vervallen. Gelukkig hebben wij een aan andere spreker bereid gevonden om de Round Table te verzorgen.
De heer Delpeut zal later dit jaar herpland worden.
Mocht het onderwerp niet in het verlengde van uw interesses liggen, dan kunt u zich afmelden via roundtables@isaca.nl.

Onderwerp: (on)mogelijkheden van CEH bij externe service providers Deel 1:
Veel organisaties willen of moeten periodiek penetratietesten op hun kritieke systemen uit (laten) voeren. Dit is een positieve en noodzakelijke(!) ontwikkeling om kwaadwillende, creatieve hackers zo goed mogelijk buiten de deur te kunnen houden. Met de groei van de markt bieden meer en meer partijen zich aan die penetratietesten uitvoeren. De kwaliteit van deze partijen, hun tools en het aanvalsplan moet voorafgaand aan de test worden vastgesteld. Best ingewikkeld, vooral omdat deze tests steeds vaker worden uitgevoerd op systemen die onderdeel zijn van lange en complexe ketens en infrastructuren. Daarbij zijn bijna altijd derde partijen betrokken. Deze Service Providers leveren meestal – min of meer - 'shared services' (b.v. cloud). De service provider is dus altijd verantwoordelijk voor de continuïteit van de dienstverlening voor meerdere klanten. En moet voorkomen dat de integriteit en beschikbaarheid van systemen negatief wordt beïnvloed door (de mogelijke bijwerkingen van) een penetratietest. Daarnaast zijn er ook nog wat juridische te regelen om te voorkomen dat activiteiten plaatsvinden die in strijd zijn met contractafspraken of wet- en regelgeving.

Service Providers zijn ook gebaat bij deze periodieke security tests. Atos heeft daarom een juridisch en operationeel model ontwikkeld waarmee deze tests – ondanks de complexiteit – kunnen worden gefaciliteerd. Voorafgaand aan de test worden concrete afspraken vastgelegd tussen alle partijen: klant, pentester en de service provider. Inmiddels is het model al zo'n 3 jaar in gebruik en geaccepteerd door verschillende partijen op de Nederlandse markt. Paul Oor (Chief Security Officer Atos BeNeLux & Nordics) en Arthur Meulstee (Senior Manager Advanced Security Center EY) laten u op basis van concrete voorbeelden en scenario's graag zien wat de (on)mogelijkheden zijn en geven concrete handreikingen om de uitvoering van penetratietesten op een goede manier te faciliteren.

Over de spreker:
Paul W.M. Oor (CISSP, CISM, CIPP/E) is samen met zijn collega's als Chief Security Officer verantwoordelijk voor security binnen Atos Benelux & The Nordics. Het mogelijk maken van security tests door derde partijen op verzoek van klanten uit allerlei markten en sectoren is een belangrijk onderdeel van zijn werkzaamheden geworden. Net als zijn collega's is hij doordrongen van het nut en de noodzaak van deze tests en zoekt daarom doorlopend naar opties om die vanuit juridisch en operationeel perspectief met een standaard aanpak te faciliteren.

Met vriendelijke groet,

Jos Maas
ISACA NL Chapter