four lines of defence for safe data

experiences in auditing information security

Dr. R. Willemse, Court of Audit of Rotterdam
International Seminar Eurorai
19th of April, 2018

why auditing information security?

- local authorities more and more work with highly sensitive information
- growing attention for privacy; new regulations (GDPR)
- In Rotterdam big data leak, also of councillers!
- formal request of council for audit

three audit perspectives

- has executive board formulated an adequate policy?
- is this policy implemented well?
- does it work?

formulation and implementation

- well formulated policy
  → risk analyses
  → privacy impact assessments
  → pdca-cycle

- not adequately implemented

does information security policy really work?

four different tests:

- external penetration
- internal penetration
- walking in
- social engineering

performed by specialized bureau (ethical hackers)

Rekenkamer
ROTTERDAM

FIRST line of defence: secure your systems from outside intruders

how to test:

- externally from the internet, outside municipal offices
- without notification!

few vulnerabilities:

- non secured websites
- outdated web mail installations

Rekenkamer
ROTTERDAM

:: Welcome to EURORAI's w

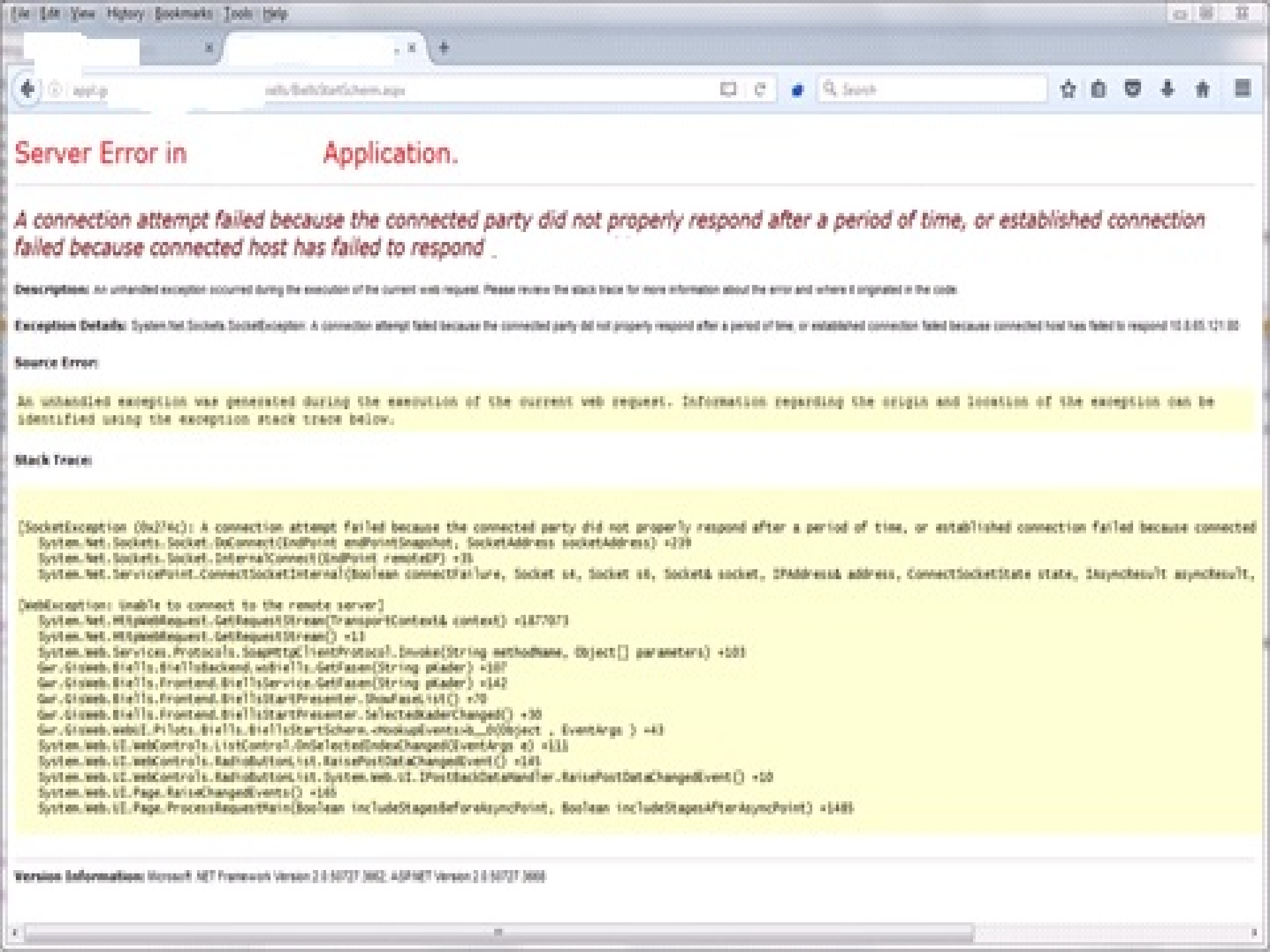
www.eurorai.org

EURORAI

EUROPEAN ORGANISATION OF REGIONAL EXTERNAL PUBLIC FINANCE AUDIT INSTITUTIONS
ORGANIZACIÓN EUROPEA DE LAS INSTITUCIONES REGIONALES DE CONTROL EXTERNO DEL SECTOR PÚBLICO
EUROPÄISCHE ORGANISATION DER REGIONALEN EXTERNEN INSTITUTIONEN ZUR KONTROLLE DES ÖFFENTLICHEN FINANZWESENS
ORGANISATION EUROPEENNE DES INSTITUTIONS REGIONALES DE CONTROLE EXTERNE DES FINANCES PUBLIQUES
ЕВРОПЕЙСКАЯ ОРГАНИЗАЦИЯ РЕГИОНАЛЬНЫХ ОРГАНОВ ВНЕШНЕГО ФИНАНСОВОГО КОНТРОЛЯ

Welcome to EURORAI's website
Bienvenidos a la página web de EURORAI
Willkommen auf den Internetseiten von EURORAI
Bienvenus sur le site Internet d'EURORAI
Добро пожаловать на вебсайт ЕВРОРАИ

| English | Español | Deutsch | Français | Русский



Server Error in Application.

A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond .

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 10.0.65.121:80

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

[SocketException (0x274c): A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected
System.Net.Sockets.Socket.DoConnect(EndPoint endPointSnapshot, SocketAddress socketAddress) +139
System.Net.Sockets.Socket.InternalConnect(EndPoint remoteEP) +35
System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address, ConnectSocketState state, IAsyncResult asyncResult,

[WebException: Unable to connect to the remote server]
System.Net.HttpWebRequest.GetRequestStream(TransportContext& context) +1877977
System.Net.HttpWebRequest.GetRequestStream() +11
System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(String methodName, Object[] parameters) +101
Gwr.Gisweb.Biells.BiellsBackend.wsBiells.GetFasen(String pLader) +107
Gwr.Gisweb.Biells.Frontend.BiellsService.GetFasen(String pLader) +142
Gwr.Gisweb.Biells.Frontend.BiellsStartPresenter.ShowFaseLivi() +70
Gwr.Gisweb.Biells.Frontend.BiellsStartPresenter.SelectedRaderChanged() +30
Gwr.Gisweb.webUI.Pilots.Biells.BiellsStartSchera.<HookupEvents>b__0(Object , EventArgs) +43
System.Web.UI.WebControls.ListControl.OnSelectedIndexChanged(EventArgs e) +111
System.Web.UI.WebControls.RadioButtonList.RaisePostDataChangedEvent() +101
System.Web.UI.WebControls.RadioButtonList.System.Web.UI.IPostBackDataHandler.RaisePostDataChangedEvent() +10
System.Web.UI.Page.RaiseChangedEvents() +105
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1481

Version Information: Microsoft .NET Framework Version:2.0.50727.3662; ASP.NET Version:2.0.50727.3668

SECOND line of defence: secure your systems from inside intruders

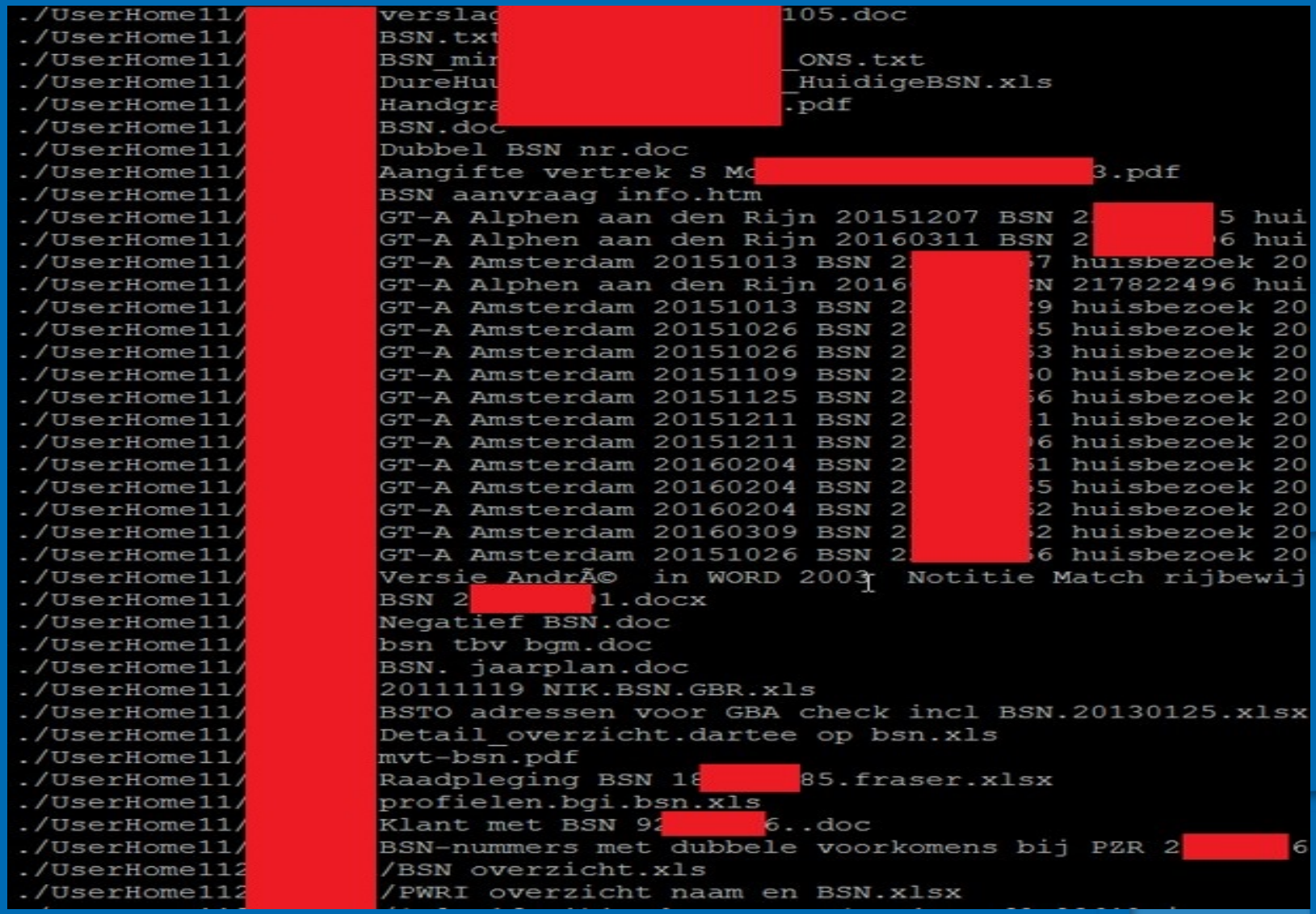
how to test:

- inside the municipal offices, with own devices
- trying to hack with or without given account/password
- again: without notification

severe vulnerabilities

- able to detect administrator’s password
- no segmentation
- able to get in everywhere, to do everything

Rekenkamer Rotterdam



Rekenkamer
ROTTERDAM

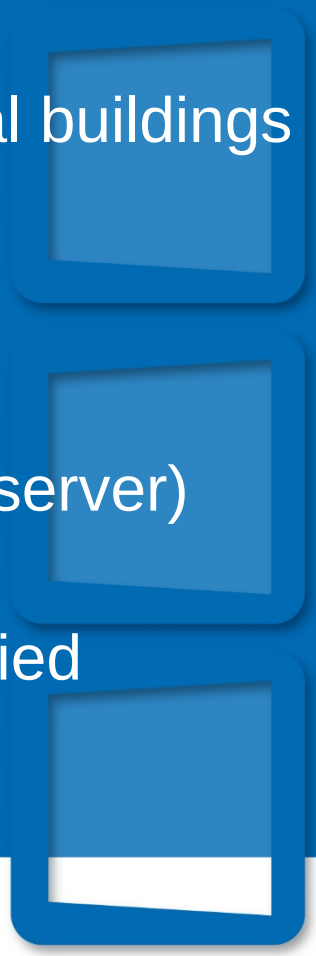
THIRD line of defence: do not let outside intruders get in physically

how to test:

- try getting unauthorized access to municipal buildings

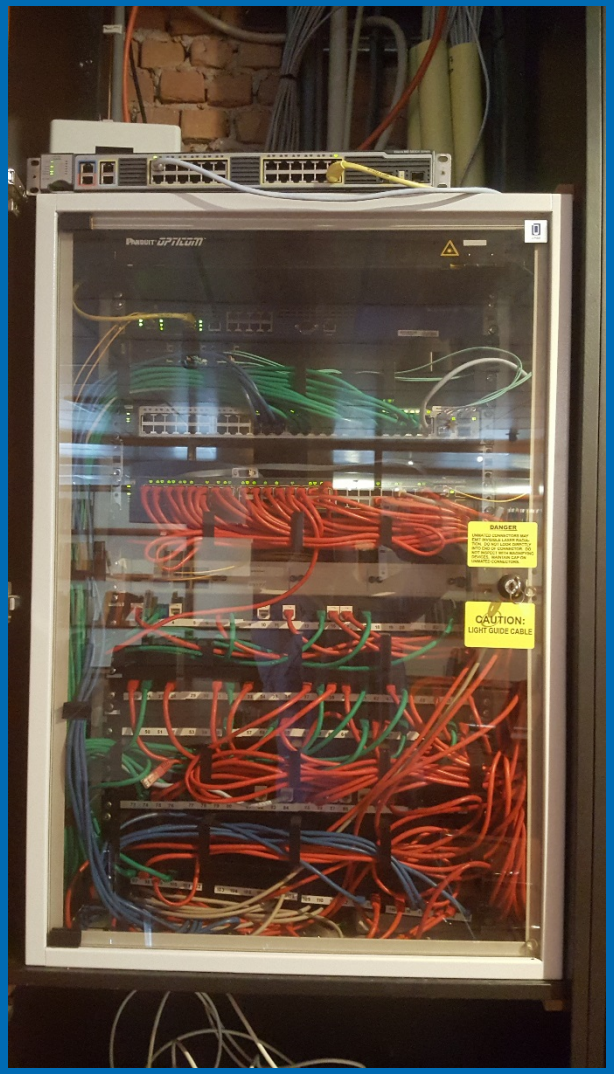
easy to get in:

- in every tested building
- access to sensitive paper documents and (server) rooms
- never stopped, sometimes even accompanied



Rekenkamer Rotterdam

Rekenkamer
ROTTERDAM



Rekenkamer
ROTTERDAM

FOURTH line of defence: strengthen awareness of employees

how to test

- drop contaminated usb-sticks (in combination with walk in tests)
- spear phishing
- voice phishing

awareness not strong

- several sticks opened
- infected links opened

To: [redacted]

Show details

Beste meneer of mevrouw,

De stichting Revalderende Vrienden zou graag een keer een rondleiding op het stadhuis genieten. De groepen en enkele voorgestelde dagen/weken zijn bijgesloten in de spreadsheet.

Omdat deze persoonsgegevens bevat is deze beveiligd met het wachtwoord:

#Samsung2k16

Kunt u laten weten of de voorgestelde bezoeken binnen uw agenda passen?
Alvast bedankt.

Met vriendelijke groet,

John Muller
jpmuller@protonmail.com
+31 6 8299 4245
Sent with ProtonMail Secure Email.

88.1 KB 1 file attached

Rekenkamer
ROTTERDAM

overall conclusion

- **despite rather well protection against external intrusions, still combination of:**

  - failing security against attacks from inside
  - failing physical security
  - too little security awareness employees

Rekenkamer
ROTTERDAM

implications

- **failing security not just technical issue or administrative problem**

- **implies severe risks on:**
  - identity fraud
  - physical unsafety public officials
  - disturbance of public order
  - sabotage of public services
  - misuse of public resources

finally

- **discussion on publication results**
- **principle of responsible disclosure**
- **follow up audit after year:**
  - hackers did not succeed in getting in
  - physical security improved
  - much stronger awareness employees
- **initial audit very effective**