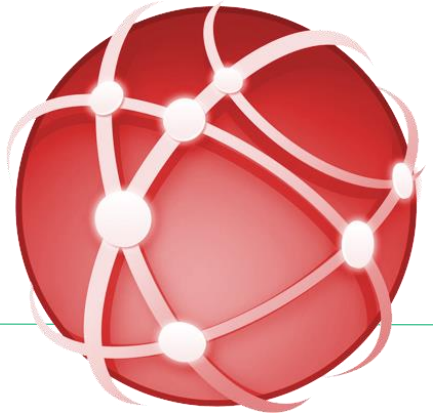
ERNW
providing security.

Designing State-of-the-Art Business Partner Connections



Enno Rey, erey@ernw.de
Matthias Luft, mluft@ernw.de

ERNW GmbH

Heidelberg/Germany based security consulting and assessment company.

- Independent
- We understand corporate
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations

- Blog: www.insinuator.net
- Conference: www.troopers.de

Agenda

- Problem Statement
- Connection Approaches
- Case Study

Problem Statement

- Pretty much every organization has an – ever growing – number of "external connections".
  - Business partners
  - Joint ventures
  - Industry consortia
  - Mergers & acquisitions etc.
- Some organizations might have an inadequate tool set for dealing with those.

What Do You Mean by "Inadequate"?

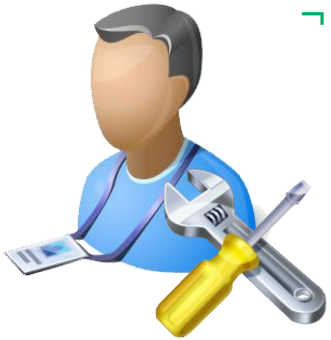
- Inefficient
  - Spending (protection) resources where not needed.
- Inflexible
  - Hindering/impacting business.
  - Hence creating discussions and (too) many *risk acceptance* procedures.
- Insufficient
  - Very often, just technical controls on the network layer ("2-staged firewall") applied. But (infosec) life is more than just firewalls ;-)

Efficiency

ISO 9000:2005: "relationship between the result achieved and the resources used"

- "result"

  = risk reduction



- "resources"

  = (mainly) operational expenditure (OPEX) of security processes

Approaches that We See out There

- "Criteria"-based
  - Look at some parameters and classify accordingly, usually in a very simple way.
- Risk-based
  - Evaluate risk associated with $CONNECTION and act accordingly.
- Questionnaire-based
  - Ask some questions and then decide somehow/apply sth.

Criteria-based

- Number/percentage of shares controlled
- Security parameters of $OTHER_NETWORK
- Certifications (e.g. ISO 27001)
- Location/legal venue?
- Who controls/operates systems?

Criteria-based

Pros & Cons

- Simply doesn't work in VUCA world.

Risk-based approach

"The domains should be defined based on a risk assessment and the different security requirements within each of the domains."

ISO 27002, 11.4.5 Segregation in networks

- In the end of the day it's about only one question:

To what extent does the business risk change?

Threats	Probability	Vulnerability	Impact	Risk
Malware Spread	2	3	3	18
Targeted attack from compromised host in remote network	2	3	4	24
Network connection leading to opportunities of eavesdropping on/hijacking of sensitive traffic (restricted, PII)	3	4	4	48
Introduction of untrusted networks (e.g. WLANs with insufficient crypto)	2	2	2	8
Backdoor internet access leading to undesired traffic profile or attack opportunities	3	3	2	18
Unmanaged components leading to loss of mgmt/visibility	3	2	3	18
Network troubles due to address space collisions, routing protocol interference etc.	2	2	5	20
Overall security stance of existing services in local network degraded (e.g. SMB dialect downgrade)	1	3	3	9
Insufficient logging/monitoring/auditing leading to regulatory non-compliance	2	2	5	20
Violation of regulations (e.g. personal data/PII processed in Non-EU countries without adequate protection level)	3	3	5	45

Risk-based

Sample

Risk-based

Pros & Cons

- Requires high maturity as for risk assessment/management.
  - Still, in the end of the day it's all about risk. Read: if you do this right, this is probably the best thing you can do.
- Might be subject to interpretation and subsequent "overruling" by C-Level though
  - "You didn't get the numbers right. Let me change the result for you."

Questionnaire-based

"Ask some questions and act accordingly"

- This is what most organizations do somehow.

Questionnaire-based

Pros & Cons

- Might require significant effort for data gathering.
- Often only focuses on $OTHER_ORG's security posture, but not on type of connection or data accessed.
- Crucial question: what's the result, in terms of $CONTROLS, of this procedure?
  - In many cases still "put them behind business partner firewall". or not.

What One Might Really Need

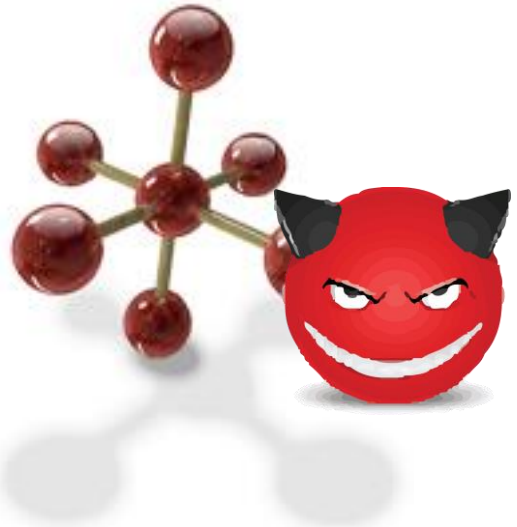
Not all Business Partners Are Equal

- Proper classification.
  - Not just good/bad or trusted/untrusted, but "how good/bad/trusted/untrusted".
  - Combined with proper set of flexible controls.
- Classification as a basis for efficient use of resources.

Let's Re-Think the Quest-based Approach for a Second

- In the end of the day, it's about classification.
  - Classification
  - Applying $CONTROLS to $CLASSES
- Ideally in a way that
  - Does not consume too many resources.
    → Limit no. of questions!
  - Does not significantly increase overall complexity.
    - Keep RFC 3439 in mind ;-)
  - Allows for reasonable application of $CONTROLS.
  - "Users" understand approach. And the questions!
- Sounds simple, right?

The Devil is in the Detail



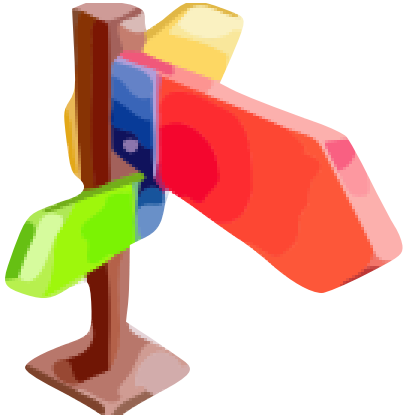
- Which classes?
- Which questions to determine classes?
- How does class determination/mapping work?
- Which controls to apply to classes?

Taking a Closer Look

- Pretty much all questions to be found in such questionnaires are related to one of the following three fundamental properties:
  - Protection need
  - Exposure (of business partner or [type of] connection).
  - Trustworthiness

So why not take those as class-defining properties?

- Overall gives max. eight (2^3) classes.
  - Could be four if all BPs regarded equally (un-) trustworthy.
- Every connection *will* belong into one of those categories.
  - One way or the other ;-)



So what has to be done

- Map questions to fundamental properties.
- Assign points
  - If you want a flexible scheme, which reflects life's diversity, points based probably the only reasonable way to go.
- Calibrate

How this Might Look in Real-Life

We're willing to share the spreadsheets shown. Please contact us by email.

Invitations for a beer are welcome, too ;-)

Business Partner Details	
Please provide details as for the company type and ownership of $ORG.	Details provided.
More specifically: does $COMPANY hold shares of $ORG?	Don't know.
Who currently manages the IT infrastructure of $ORG?	$ORG's own IT department.
Does $ORG dispose of security relevant (e.g. ISO 27001) certifications or are they willing to provide SAS 70/ISAE 3402/SSAE 16 ("Type 2") reports?	Yes, relevant reports (SAS 70 etc., "Type 2") provided l
What is – from your perspective – $ORG's maturity level as for information security management, processes and overall posture?	Overall lower than $COMPANY standards (pls explain/

Real-life Sample

Continued

Connection Details	
How long will the connection be needed?	Limited period of time (pls specify).
Which $COMPANY resources does $ORG need to access?	Broad access to resources/network needed.
Does a risk assessment for the mentioned ($COMPANY) resources exist?	No.
What is the highest (data) classification level that $ORG needs access to?	Confidential
What is the highest (data) classification of data stored on systems that $ORG accesses by some means (even if this data is not part of the planned access)?	Confidential
Will data be accessed/processed that is covered by regulatory frameworks [e.g. Data Protection, PCI, ICOFR].	Don't know.
What would – from your perspective – be the impact for $COMPANY in case the data in question was disclosed to unauthorized 3rd parties?	Financial loss / loss or revenue < 250.000 EUR (pls provide
What would – from your perspective – be the impact for $COMPANY in case the data in question was irreversibly destroyed?	Regulatory exposure/violation of laws or contracts (pls spec
What would – from your perspective – be the impact for $COMPANY in	

Real-life Sample

Continued

Can you specify *in which part(s) of the CN network* the resources to-be-accessed are located?	One or more DMZ(s) only
Does the connection terminate solely (with)in a DMZ or are the potential connection endpoints located in other parts of the $COMPANY network (e.g. CN or SSA)?	In other parts of the network (e.g. CN or SSA) as well
Can you specify how (e.g. web-related method like HTTP[S], [Windows] network share[s] etc.) the $COMPANY resources will be accessed?	Other (pls specify).
Who – from your knowledge – initiates the individual network connections/r	Only outbound connections (leaving from $COMPANY network) are needed.
Can you specify the level of privileges $ORG will need/dispose of as for the $COMPANY resources/services accessed?	Don't know.
Will the connection include the interconnection/synchronization of authentication frameworks/infrastructures (e.g. federated identities, Windows AD trusts etc .)?	No.
Does the connection include machine-to-machine communication (e.g. batc	Don't know.
Does the connection include man-to-machine communication (e.g. [human] users accessing a service or logging into $COMPANY systems)?	No man-to-machine communication planned.
Which – from your understanding – types of authentication can be used to authenticate those users if needed, both on the network or on the application level?	None.
Does the project already include a proposal/suggestion as for the type of connection (VPN, leased line, terminal services/Citrix etc.) that is supposed to be used?	No, no such proposal is included in the project.
Is a security concept part of the project that involves or triggered the conne	Don't know.

Real-life Sample

Continued

E	F	G
Trust	Exposure	Protection Need (of Resources)
2		
0		
0	2	
3	-1	
0	3	
	-2	
0	5	
	2	
		7
Low	Low	High

Mapping to $CONTROLS

	trust	exposure	protection need	Samples/ Comments
Type 1	high	low	low	mostly BusApp ("we trust Bloomberg, but we don't let them heavily into our network and the stuff is not highly sensitive anyway"), maybe some other cases
Type 2	high	high	low	might not occur very often in real life.
Type 3	high	low	high	probably default case of TBP ("they would't be a 'trusted business partner' if we assumed they were heavily exposed").
Type 4	high	high	high	scenario might occur after M & A ("we now own [& hence trust] them; they need access to our databases, ERP & AD; but they still have there own, legacy [=> 'exposed'] IT") or in joint ventures.
Type 5	low	low	low	ExtAccess
Type 6	low	high	low	common EBP case (don't trust them, expect the worst as for their exposure, do not let them access sensitive stuff).
Type 7	low	low	high	EBP with limited access (thus limited exposure, at least on our side) but needing access to some sensitive stuff (e.g. PII).
				EBP, with strong controls - or, in reality, risk acceptance - needed then. Might occur after M & A ("now somebody else owns them and

Mapping to $CONTROLS

Sample, Continued

Contractual	*Technical*				*Organizational*			
Contractual Controls	**Number & Type of Sec GWs**	**IDS/IPS**	**Encryption**	**Logging & Analysis**	**Security Testing (Pentest/Audit) of controls**	**(Need for) Connection and Controls Review**	**Risk Acceptance must be signed by**	**Ma (te**
recommended	-	-	strongly recommended	-	-	recommended every 60 months	manager level	
needed	depends / tbd	-	mandatory	-	recommended every 60 months	recommended every 36 months	depends / tbd	
strong needed	single layer recommended "for compliance reasons"	recommended if doable with reasonable effort	mandatory	recommended, for compliance reasons	recommended every 36 months	recommended every 36 months	director level	
strong needed	single layer recommended "for compliance reasons"	recommended if doable with rea-sonable op_effort	mandatory	recommended	recommended every 36 months	mandatory every 12 months	BU VP level	two + fv
recommended	recommended if doable with reasonable effort	-	recommended	-	recommended every 60 months	recommended every 24 months	director level	
needed	one layer mandatory + one additional control recommended	recommended if doable with rea-sonable op_effort	mandatory	strongly recommended	recommended every 36 months	mandatory every 24 months	director level	
	one layer							

ERNW
providing security.

Summary

- In many organizations the growing number of external connections requires appropriate tool set.
- Proper classification is key, combined with flexible set of controls.
- Finding the right balance might be a challenge. Still it can be done.

There's never enough time...

THANK YOU...

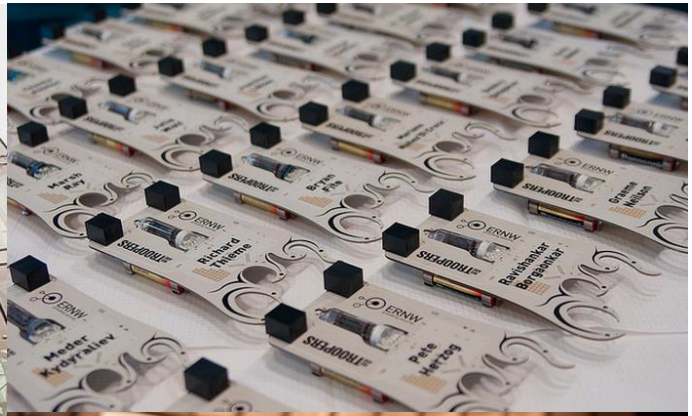
...for yours!

Questions & Discussion

Join us for TROOPERS14

ERNW
providing security.

Workshops, Conference, Roundtables, PacketWars Hacking Contest, 10k Morning Run, …



March
17th-21st 2014

Heidelberg,
Germany

www.troopers.de