

How secure is your Network ?
15 questions you need to ask your system administrator

Innominate Security Technologies AG

Rudower Chaussee 29

12489 Berlin / Germany

Tel.: +49 30 6392-3300

info@innominate.com

www.innominate.com

The following questions are based on the day by day experience of our network experts dealing with customers network security problems. Your answers should help you to get an overview about your current network security situation. In no way this replaces a professional consulting. We would also recommend consulting if you cannot answer all the questions or if the terms used are unknown to you.

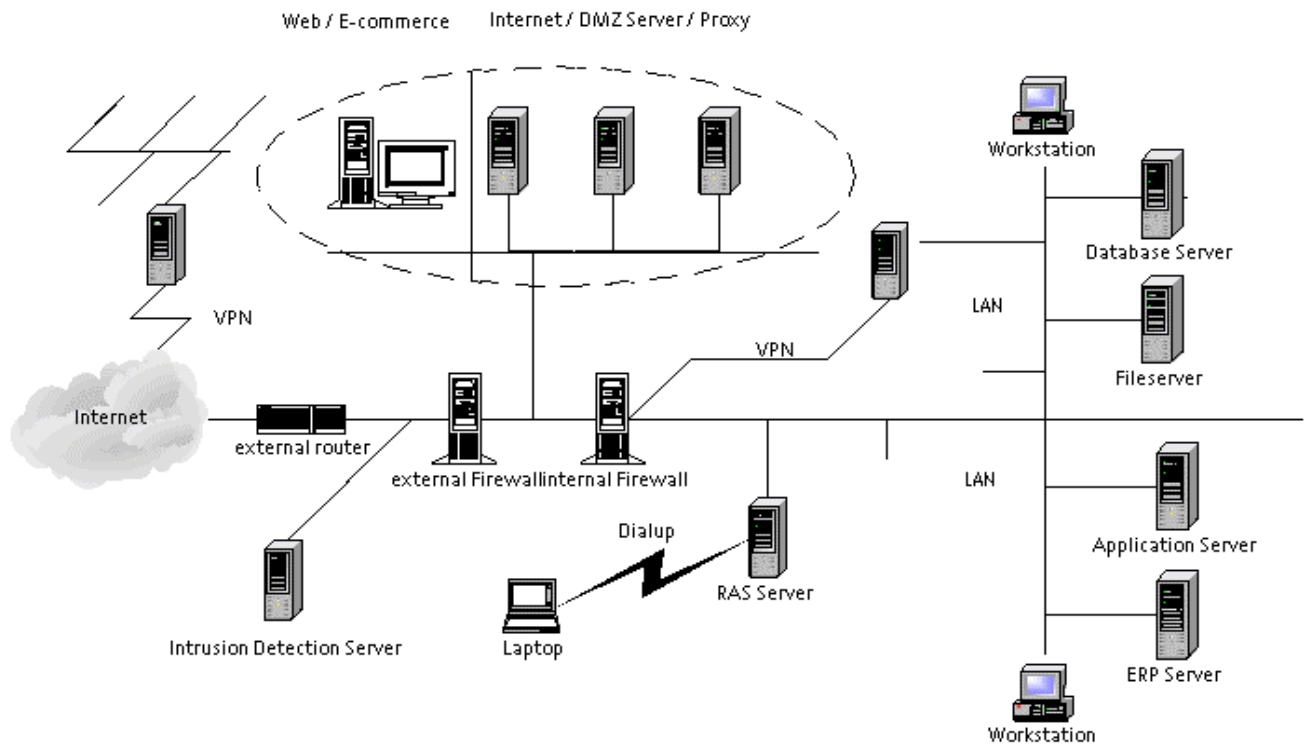
An analysis of your security requirements begins always with a threat analysis.

You need to know who may attack you, what kind of technique is used, which assets you need to protect and what would be the risk when you network is compromised.

Thread analysis is most important but not covered by his paper. The following describes technical aspects to be considered. It is up to you to decide what is valid for you.

Sensitive areas of enterprise network

This example of a network plan visualizes sensitive areas:



Security relevant areas:

1. Router Configuration

- (a) Did you change all standard passwords set by the manufacturer so that only authorised persons have access ? (Router, Switches, Network Printers)

- (b) Are the firewall rules and ACLs (Access Control Lists) of your routers verified ? (Is an unauthorised penetration of your DMZ possible?)

- (c) Is the functionality of your firewall regularly checked from the outside of your network ?
- (d) Are your firewall rules and router ACLs validated with your security policies?

2. Remote Access Services

- (a) Do you have encrypted remote access to you network so that no passwords and data can be intercepted ? (VPN, SSL, SSH)
- (b) Is your remote access service monitored ? (to prevent DOS-attacks, Brute force attacks)
- (c) Do you check all your clients regularly for trojans and viruses?
- (d) Do you have any undocumented Internet, RAS or modem connections which are not protected by a firewall ?
- (e) Do you have an escalation plans for stolen laptops or passwords?
- (f) Have your mobile computers an encrypted file systems to store sensitive files of your company?

3. Trust between Servers

- (a) Are your trusted domain structure of your NT-Servers documented ?
- (b) Do you have a set of rules for your trusted structure ?

(c) Do you have unverified unix .rhosts, .equiv files ?

(d) Do you use unencrypted tools for administration ? (telnet, rlogin, http, webmin or linuxconf)

4. User Accounts

(a) Are there any user accounts with too many privileges ?

(b) Are your test- , "dummy-" and other accounts with special rights monitored ?

(c) Do you have existing rules, which define the access rights for each user?
Are these rules validated regularly ?

(d) What happens to a user-account if someone leaves your company ? Do you have a defined procedure?

5. Application Software

(a) Do you regularly update your application software ? (Security Patches)

(b) Do you know all common software bugs in your office- and server software you have installed ?

(c) Are the default settings of your software checked against security holes ?

6. Missing/used Working instructions

- (a) Do you have published security instructions ?
- (b) Do your employees know about the security instructions ?

7. Network File System

- (a) Are access rights for each user defined and validated so only authorised user have access to important data (even unimportant information can help hackers)
- (b) Do you have unprotected public accessible files?

8. Netzwerktraffic

- (a) Do you encrypt your network traffic so nobody can sniff other peoples password ?
- (b) Is you email traffic encrypted ?

9. Passwords

- (a) You have procedures, which make it impossible for users to use weak passwords? (passwords which are not possible to guess)
- (b) Do you have common, well known standard passwords ?

- (c) Do you store your passwords at a secure place ? (Do not use sheet of paper at your monitor)

10. Wrong configured Internet services

- (a) Have you audited your CGI-scripts against security holes ?
- (b) Are there any unnecessary FTP services in your network ?
- (c) Do you make security updates on your Internet servers regularly ?

11. Firewall

- (a) Are your firewall rule sets checked regularly to respond to the changes in your network ?
- (b) Do you allow direct access to your DMZ ?
- (c) Do you have a protection against the access of trojaned servers in your DMZ

12. Network services

- (a) Do you run unnecessary services, like RPC, FTP, DNS, SMTP, BOOTP, TFTP ?

13. Blackbox

- (a) Are all the information provided by network services access protected to restrict hack attempts ? (disguise your server software version)
- (b) Do you have protection mechanisms against unauthorised connections with SNMP, finger, SMTP, telnet, rusers, rpcinfo, NetBios, DNS services ?

14. Logging

- (a) Do you have logging mechanisms that log attacks ? Are these logs suitable for court ?
- (b) Do you pursue hackers/hack attempts ?
- (c) Do you have network accounting, to localise attacks from inside your network ?
- (d) Do you have an intrusion detection system ?
- (e) Do you have mechanisms to alert you administrators ? (Mail, pager, Fax, Voice) to have a quick response to hackers ?

15. Virus protection

- (a) Are your Clients virus patterns updated regularly ?
- (b) Do you have virus protection on your Internet gateway ?

(c) Are all incoming and outgoing emails scanned for viruses and Trojans ?

(d) Are you file servers scanned for viruses regularly ?

(e) Do you have an automated daily update for your virus protection ?