SURVEY ON NETWORK ATTACK DETECTION AND MITIGATION

CASED

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP
http://www.dasec.h-da.de/

Welcome to the da/sec survey on network attack detection and mitigation. Network-based attacks pose a strong threat to the Internet landscape and academia is working towards different approaches on attack detection and mitigation. Yet, a clear understanding of possibilities and issues in commercial networks is missing. Hence, this survey aims at gaining insight in real-world processes, structures and capabilities of IT companies and the computer networks they run. This survey is conducted in context of different publicly funded research projects and work done in the combined eco e.V. and DE-CIX competence group security. Results of this survey shall frame future research and community activities in the area of Internet security.

The survey targets at companies of all size and color running an own computer network. Questions within this survey address some organizational aspects, as well as processes, techniques and tools you may have employed in order to perform network attack detection and mitigation. **Filling the survey should not last longer than 5 - 10 minutes.** Hence, the survey can ideally be answered during a short and relaxing coffee break.

The survey is completely anonymous. We will not require you to enter any personally identifiable information, neither will log IP addresses with your responses. Nevertheless, you will have the possibility to voluntarily provide us your email address and/or name. If you do so, you give us the possibility of getting in touch with you in case of any open questions.

Thank you very much for taking your time to support our work!

There are 56 questions in this survey

Company and personal information

The following questions will ask some general questions regarding your company and your role within your company. Answering these questions allows us to draw more fine-grained conclusions on the survey.

Questions marked with asterisk (*) are required.

1. What is your role within your company? *

Please choose **only one** of the following:

- ○ Network operator or engineer
- ○ Security operator or engineer
- ○ Data protection officer / Information security officer
- ○ Management
- ○ Other:

2. How would you classify your company? *

Please choose **only one** of the following:

- ○ Carrier/Telco/ISP
- ○ Hosting/Data Center/Colocation Services Provider
- ○ Research and Education Network
- ○ CDN/Content Delivery
- ○ Cloud Services Provider
- ○ Enterprise
- ○ Other:

3. Where is your company headquartered? *

Please choose **only one** of the following:

- ○ Africa
- ○ America
- ○ Asia
- ○ Australia
- ○ Europe

4. Let *x* denote the monthly average traffic rate transported within your company's network. What approximates *x* best?

Please choose **only one** of the following:

- ○ 0 < x <= 1 Gbit/s
- ○ 1 < x <= 5 Gbit/s
- ○ 5 < x <= 10 Gbit/s
- ○ 10 < x <= 50 Gbit/s
- ○ 50 < x <= 100 Gbit/s
- ○ > 100 Gbit/s

Make a comment on your choice here: [ ]

This question is optional. Giving an answer to this question will help us to correlate answers to upcoming questions with the size of a network, as we believe that monthly average traffic rate serves as a good measure of network size. If you'd disagree, we'd be happy to learm from your comments!

5. **Does your company have a dedicated security department that handles network security events (e.g. compromised servers, DoS attacks)? ***

Please choose **only one** of the following:

- ○ Yes
- ○ No

6. **Let *x* denote the size of your company's security department. What approximates *x* best?***

Please choose **only one** of the following:

- ○ 0 < x <= 2
- ○ 2 < x <= 5
- ○ 5 < x <= 10
- ○ 10 < x <= 20
- ○ 20 < x <= 50
- ○ > 50
- ○ Do not know

7. **Does your company have a dedicated department that handles customer security events (e.g. bot infected devices)? ***

Please choose **only one** of the following:

- ○ Yes
- ○ No

8. **Let *x* denote the size of your company's department that handles customer security events. What approximates *x* best? ***

Please choose **only one** of the following:

- ○ 0 < x <= 2
- ○ 2 < x <= 5
- ○ 5 < x <= 10
- ○ 10 < x <= 20
- ○ 20 < x <= 50
- ○ > 50
- ○ Do not know

9. Does your company employ measures to *pro-actively* detect Internet attacks?

Please choose **only one** of the following:

- ○ Yes
- ○ No

10. Does your company *plan to* employ measures to be able to *pro-actively* detect Internet attacks in *future*?

Please choose **only one** of the following:

- ○ Yes
- ○ No

11. Does your company employ measures to correlate security events?

Please choose **only one** of the following:

- ○ Yes
- ○ No

12. Does your company adhere to IT process or security frameworks and/or standards?

Please choose **all** that apply:

- ☐ Yes, ITIL
- ☐ Yes, COBIT
- ☐ Yes, ISO/IEC 27000 (e.g. 27001, 27002)
- ☐ Other:

Attacks and threats

The following questions will cover attacks and threats that you may have faced or fear to face.

Questions marked with asterisk (*) are required.

13. What raises your awareness of Internet attacks? *

Please choose **all** that apply:

- ☐ Your company's infrastructure had been under attack
- ☐ Your company's customers have been under attack
- ☐ Legal and/or regulatory requirements
- ☐ Publications in journals, magazines, web sites and mailing lists
- ☐ Presentations and discussions on conferences
- ☐ Other:

14. How do you inform yourself and keep track of new types of attacks and threats? *

Please choose **all** that apply:

- ☐ Mailinglists
- ☐ Security conferences
- ☐ Web sites/blogs/syndication feeds
- ☐ Social networks
- ☐ Vendors
- ☐ Scientific publications
- ☐ Other:

15. **How would you rate the risk the following threats pose to your company's infrastructure?*** Please choose the appropriate response for each item:

	Very low	Low	Medium	High	Very high	Do not know
Misconfiguration of network equipment and servers	○	○	○	○	○	○
Compromised and/or bot infected devices within your network	○	○	○	○	○	○
Compromised and/or bot infected devices outside of your network	○	○	○	○	○	○
Targeted attacks / zero-day exploits	○	○	○	○	○	○
Denial of service attacks	○	○	○	○	○	○
Malware	○	○	○	○	○	○

16. **How would you rate the risk the following threats pose to your company's customers? *** Please choose the appropriate response for each item:

	Very low	Low	Medium	High	Very high	Do not know
Misconfiguration of network equipment and servers	○	○	○	○	○	○
Botnets	○	○	○	○	○	○
Drive-by downloads	○	○	○	○	○	○
Targeted attacks / zero-day exploits	○	○	○	○	○	○
Denial of service attacks	○	○	○	○	○	○
Malware	○	○	○	○	○	○
Information theft	○	○	○	○	○	○

17. Let *x* denote the number of attacks targeting your company's infrastructure and customers per month on average. What approximates *x* best?*

Please choose **only one** of the following:

- ○ 0 < x <= 10
- ○ 10 < x <= 20
- ○ 20 < x <= 50
- ○ 50 < x <= 100
- ○ 100 < x <= 250
- ○ 250 < x <= 500
- ○ > 500
- ○ Do not know

Data and tools

The following questions will cover data and tools your company uses for attack detection and mitigation. Questions marked with asterisk (*) are required.

18. Which type of tools does your company use for attack detection? *

Please choose **all** that apply:

- ☐ Commercial products
- ☐ Opensource software
- ☐ Self-build tools

19. Which type of tools does your company use to correlate security events? *

Please choose **all** that apply:

- ☐ Commercial product
- ☐ Opensource software
- ☐ Self-build tools

20. Does your company have the technical ability to perform network wide deep packet inspection?

Please choose **only one** of the following:

- ○ Yes
- ○ No

With 'technical ability' we mean: is it, from a technical point of view, possible to perform network wide deep packet inspection. I.e. have you the possibility to deploy tap devices? Have you the possibility to configure traffic shunts (e.g. via MPLS)? Can you configure port mirroring?

If your answer to one or more of these exemplary questions is 'yes', we would call this a 'technical ability' to perform network wide deep packet inspection.

21. Do you think it is *feasible* for your company to perform network wide deep packet inspection? *

Please choose **only one** of the following:

- ○ Yes
- ○ No

22. Why do you think network wide deep packet inspection is not feasible? *

Please choose **all** that apply:

- ☐ Requires too much human resources (OPEX)
- ☐ Financial invest to high (CAPEX)
- ☐ Too much network traffic to process
- ☐ Want to protect our customers' privacy
- ☐ Prohibited by legal and/or regulatory requirements
- ☐ Other:

23. Does your company employ tools to visualize network security events?

Please choose **only one** of the following:

- ○ Yes
- ○ No

24. Which tools does your company employ to visualize network security events? *

Please choose **all** that apply:

- ☐ ArcSight
- ☐ AfterGlow
- ☐ PixlCloud
- ☐ Self-build tools
- ☐ Other:

25. Which kind of data does your company *currently* use for attack detection? *

Please choose **all** that apply:

- ☐ SNMP data
- ☐ sFlow data
- ☐ NetFlow data
- ☐ IPFIX data
- ☐ Raw packets
- ☐ Darknet / backscatter
- ☐ Mail / DNS / DHCP server logs
- ☐ Other server logs
- ☐ Other:

26. Which kind of data does your company *plan to use* for attack detection in *future*? *

Please choose **all** that apply:

- ☐ SNMP data
- ☐ sFlow data
- ☐ NetFlow data
- ☐ IPFIX data
- ☐ Raw packets
- ☐ Darknet / backscatter
- ☐ Mail / DNS / DHCP server logs
- ☐ Other server logs
- ☐ Other:

27. Does your company's infrastructure currently offer the availability to collect NetFlow data?

Please choose **only one** of the following:

- ○ Yes
- ○ No

28. Which NetFlow versions are supported in your company's infrastructure?

Please choose **all** that apply:

- ☐ NetFlow version 5
- ☐ NetFlow version 7
- ☐ NetFlow version 8
- ☐ NetFlow version 9

29. Does your company's infrastructure currently offer the availability to collect sFlow data?

Please choose **only one** of the following:

- ○ Yes
- ○ No

30. Does your company's infrastructure currently offer the availability to collect IPFIX data?

Please choose **only one** of the following:

- ○ Yes
- ○ No

31. Do you think collecting and processing NetFlow data in order to perform network attack detection protects privacy rights of your customers better than collecting and processing raw packets?

Please choose **only one** of the following:

- ○ Yes
- ○ No

Mitigation and reaction

This section covers all questions related to mitigation of and reaction on detected attacks.

Questions marked with asterisk (*) are required.

32. Which measures do you usually take to mitigate network attacks targeting at your company's infrastructure? *

Please choose **all** that apply:

- ☐ Access-control list / packet filter
- ☐ Firewall
- ☐ Intrusion Prevention System
- ☐ Source-based remote-triggered blackhole
- ☐ Destination-based remote-triggered blackhole
- ☐ Other:

33. Which measures do you usually take to mitigate network attacks targeting at your company's customers? *

Please choose **all** that apply:

- ☐ Access-control list / packet filter
- ☐ Firewall
- ☐ Intrusion Prevention System
- ☐ Source-based remote-triggered blackhole
- ☐ Destination-based remote-triggered blackhole
- ☐ Other:

34. Let x denote the number of minutes it takes to initially mitigate an ongoing attack on average? What approximates x best?

Please choose **only one** of the following:

- ○ 0 < x <= 10
- ○ 10 < x <= 20
- ○ 20 < x <= 30
- ○ > 30

35. Let x denote the number of days it takes to completely resolve attacks on average? What approximates x best?

Please choose **only one** of the following:

- ○ 0 < x <= 1
- ○ 1 < x <= 3
- ○ 3 < x <= 5
- ○ 5 < x <= 10
- ○ 10 < x <= 20
- ○ > 20

36. Does your company share attack information with 3rd parties?

Please choose **only one** of the following:

- ○ Yes
- ○ No

37. With whom does your company share attack information? *

Please choose **all** that apply:

- ☐ Customers
- ☐ Vendors
- ☐ Competitors
- ☐ CERTs
- ☐ Law enforcement
- ☐ Other:

38. How does your company exchange attack information with 3rd parties? *

Please choose **all** that apply:

- ☐ E-Mail
- ☐ Telephone
- ☐ Automated by detection system
- ☐ Other:

39. Does your company use a standardized format for automated data exchange?

Please choose **only one** of the following:

- ○ Yes
- ○ No

40. How well do you know the following data exchange formats? *

Please choose the appropriate response for each item:

	Do or did use	Known	Heard of	Unknown
IDMEF	○	○	○	○
IODEF	○	○	○	○
MARF	○	○	○	○
x-ARF	○	○	○	○
CEE	○	○	○	○
MAEC	○	○	○	○
SCAP	○	○	○	○

41. Would you consider using the following formats for data exchange? *

Please choose the appropriate response for each item:

	Yes	No	Do not know
IDMEF	○	○	○
IODEF	○	○	○
MARF	○	○	○
x-ARF	○	○	○
CEE	○	○	○
MAEC	○	○	○
SCAP	○	○	○

42. Does your company have a well-defined process for mitigation and/or information exchange? *

Please choose **only one** of the following:

- ○ Yes
- ○ No

Role of ISPs and IXPs

We would like to collect your thoughts on the role of Internet Service Providers (ISPs) and Internet Exchange Points (IXPs) in detection and mitigation of network attacks targeting your own infrastructure and customers. Questions marked with asterisk (*) are required.

43. Do you think ISPs play an important role in network attack detection and mitigation? *

Please choose **only one** of the following:

- ○ Yes
- ○ No

44. What would be the appropriate way of thinking, from your point of view? *

Please choose **only one** of the following:

- ○ ISPs shall protect its customers from Internet attacks
- ○ ISPs shall protect the Internet from attack originating from its customers

Make a comment on your choice here: [ ]

You can leave any additional opinion about that topic via the comment field.

45. Why do you think ISPs do not play an important role in network attack detection and mitigation? *

Please write your answer here: [ ]

46. Do you think there is a financial incentive to perform network attack detection and mitigation for ISPs?

Please choose **only one** of the following:

- ○ Yes
- ○ No

47. Why do you think there is no financial incentive for ISPs to perform network attack detection and mitigation? *

Please write your answer here: [ ]

48. Do you think IXPs can/could play an important role in network attack detection and mitigation? *

Please choose **only one** of the following:

- ○ Yes
- ○ No

49. Which task do you think IXPs can/could take in network attack detection and mitigation? *

Please choose **all** that apply:

- ☐ Detection / Analysis
- ☐ Mitigation / Response
- ☐ Correlation
- ☐ Coordination
- ☐ Other:

50. Why do you think IXPs can/should not play an important role in network attack detection and mitigation? *

Please write your answer here:

51. Do you think IXPs should implement measures to centrally and conditionally collect network traffic traces? *

Please choose **only one** of the following:

- ○ Yes
- ○ No

Contact information

The following questions are all optional. You have the possibility to give us some supplementary information that allow us to get in touch with you if we have further questions on your answers

52. What is the name of your company?

Answering this question is optional. Giving us the name of your company will help associating and correlating answers that might also be given by one of your colleagues on behalf of the same company.

53. What is your email address?

Answering this question is optional. Giving us your name and email address allows us to get in touch with you in person if we have some questions on your answers. If you don't want this, please simply leave the above text field unfilled.

54. What is your name?

Answering this question is optional. Giving us your name and email address allows us to get in touch with you in person if we have some questions on your answers. If you don't want this, please simply leave the above text field unfilled.

55. If you were to introduce new system capable to do pro-active network attack detection, event correlation and visualization as well as information exchange, what would be your requirements?

56. Is there any final information, hint or comment you want to give?

Please write your answer here:

Thank you for participating in this survey, we really appreciate the time you spent! If you left your personal contact information, as a little "thank you" we will send you the results of this survey after we analyzed and concluded on all answers.

If you have any questions regarding this survey or our research projects or if you'd like to further support our projects, please feel free to get in touch with sebastian.abt@h-da.de