MKB Nederland

Campaign: “Veilig zakelijk internetten”

To make entrepreneurs aware of cybercrime

Ellen Jacobs, projectmanager MKB-Nederland

Luxembourg, December 17, 2015

The Project

The challenge

Entrepreneurs are hardly aware of the impact of cybercrime on their business while:

- € 7,5 billion euros business damage per year
- The Netherlands target country for cybercrime

Our approach

- 5 roadshows in cooperation with the regional networks for safely entrepreneuring → awareness
- The offer of 300 ‘live’ hacks → a call to action!

Roadshows

- MKBuzz with IT and insurance advisor
- Information program/seminar + information market in cooperation with the local entrepreneurs associations and local authority
- Promotion team
- Media attention
- Digital magazine with interviews with experts and local authorities

MKB Nederland

Digital magazine

Index

MKB Nederland

Free ethical hack for entrepreneurs

Bescherm je bedrijf tegen cybercrime!

Laat je bedrijf hacken door een ethische hacker

Welkom op de actiepagina van de campagne Veilig Zakelijk Internetten. Deze campagne is afgerond. Tijdens deze campagne konden ondernemers zich voor een gratis ethische hack aanmelden. De initiatiefnemers van de campagne, MKB-Nederland en het ministerie van Veiligheid en Justitie, zijn de campagne in augustus 2015 gestart om ondernemers te ondersteunen hun cybersecurity te vergroten en zo cybercriminaliteit terug te dringen.

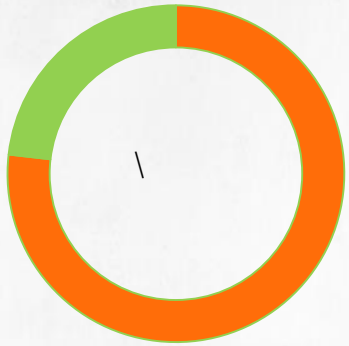
Hack results

Entrepreneurs that applied 226

Of 300

‘Hacks’

Amount of scanned hosts 535



76,82% INSUFFICIENT

23,18% SUFFICIENT

Feed back appointments

No response to invitation 91

Of 226

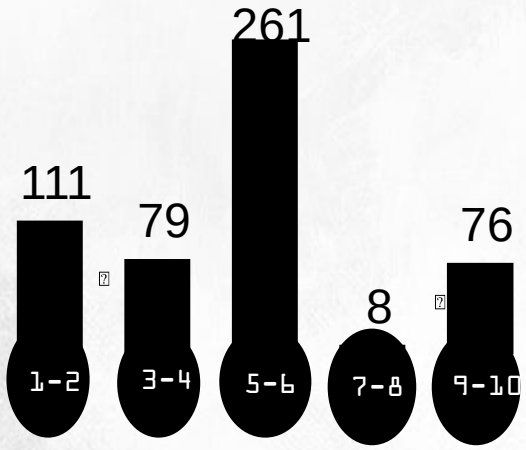
No-show at appointment 21

Of 226

Feed back conversations 114

Of 226

Hacks versus scores



	Top-5 business impact
1.	Easy access to relevant data
2.	Routers/firewalls easy to manipulate
3.	Webshops and websites badly programmed or maintained.
4.	Overdue maintenance
5.	Servers and websites already been hacked

ThreadStone CYBER SECURITY

ThreadScan scoring translation based on CVSS v3

ThreadScan Scoring	Exploit available	Description	CVSSv3 Score	Description	Action
1 2	Yes No	Poor / bad	Critical	You run a severe risk of a cyber intrusion and data leakage, urgent action by IT is required. Vulnerabilities have been discovered that can be used by cybercriminals to break into your website and/or other equipment connected to the Internet. These vulnerabilities should urgently be fixed by your IT contact to reduce the severe risk of a data leak.	Urgent action by IT required
3 4	Yes No	Insufficient	High	You run a significant risk of a cyber intrusion and data leakage, immediate action by IT is required. Vulnerabilities have been discovered that can be used by cybercriminals to break into your website and/or other equipment connected to the Internet. These vulnerabilities should be examined by your IT contact and fixed to reduce the considerable risk of a data leak.	Immediate action by IT required
5 6	Yes No	Moderate	Medium	You run the risk of a cyber intrusion and data leakage, further action by IT is required to fix vulnerabilities. Vulnerabilities have been discovered that can be used by cybercriminals to break into your website and/or other equipment connected to the Internet. These vulnerabilities should be examined by your IT contact and fixed as a measure to reduce the risk of a data leak.	Action by IT required
7 8	Yes No	Sufficient	Low	You are protected against cyber criminals, but a final check by IT is required. There are vulnerabilities discovered that cybercriminals may use to break into your website and/or other equipment connected to the Internet. These vulnerabilities should be examined by your IT contact and possibly corrected as a measure to reduce the risk of a data leak.	Action by IT required
9 10	Yes No	Good	Informational	You are well protected against cyber intrusions.	No action required.

Score	CVSSv3
Critical	9.0..10.0
High	7.0..8.9
Medium	4.0..6.9
Low	0.1..3.9
None	0

ThreadStone CYBER SECURITY

Conclusions

- SME's are positive about the campaign and especially about the free hack;
- Awareness still lacks, based on the no show at the feedback appointment (almost 50%);
- Main cause for cybercrime vulnerability: overdue maintenance;
- The most critical vulnerabilities are caused by people (lack of attention;
- IT suppliers (networkhosts, webdevelopers) are inspired to develop new services/ propositions, in the spirit of this campaign.

Top 5 causes

- Impact potential hacks is recognised insufficiently
- SME's just start acting after they have been attacked by cybercrime;
- Digital safety demands **attention, attention, training, procedures**
- **and technical investments** → average SME lacks 4 of 6;
- Lack of attention and overdue maintenance most occuring vulnerability;
- **'Gap'** between the offer of suppliers and the expectations of SME's.
- IT-suppliers experience an offer in this area as a shortcoming of
- their own services.

Evaluation

- 58% states more awareness regarding cybercrime
- 45% took measurements *after the intake* for the hack
- 1 on 5 SME's took improvements regarding WIFI and personnel IT protocol
- 25% did this *after the hack*
- 83% of the hacked SME's puts cybercrime permanently on the agenda
- 77% does not consider cybercrime insurance
- Before the hack 72% of the SME's did not put their IT network on regular check. After the hack 84% considers a regular check
-

Finally

- We did not sell all 300 hacks;
- SME's gave unsufficient priority to the feed back of 'their hack';
- 75% of the SME's that has been hacked is unsufficiently protected against cybercrime;
- The hacker business is quite inventive → every day brings new
- tricks to enter IT-enviroments.

So..

our mission to make SME's aware of cybercrime is not accomplished...yet..