Public Prosecution Service

Board of Procurators General

Prosecutor General

Postal address: PO Box 20305, 2500 EH The Hague.

Street address:
Prins Clauslaan 16
2595 AJ The Hague
Telephone +31 70 33 99 600
Telefax +31 70 33 99 851

To all chief prosecutors

Branch	Policy and Strategy
Contact person	
Direct extension(s)	
Date	18 March 2013
Our reference	PaG/B&S/16708
Supplement	1
Subject	Responsible Disclosure (how to deal with 'ethical' hackers?)

When responding please indicate the date and our reference.
Please deal with only one matter in your letter.

Dear colleagues,

Recently the National Cyber Security Centre (NCSC) of the Ministry of Security and Justice presented a guide for organisations (government and industry) and 'ethical' hackers to report and deal with vulnerabilities in information systems and in (software) products in a responsible manner. This guide is entitled: 'Guide towards a practice of Responsible Disclosure' (see supplement). The objective of this guide is to provide 'building blocks' for organisations to enable them to establish a policy for Responsible Disclosure. This policy provides the 'ethical' hacker with clarification of how the relevant organisation will deal with the vulnerabilities in the ICT systems revealed and/or reported by this hacker, and it offers affected enterprises the opportunity to remedy vulnerabilities and to limit damage before the hacker goes public with his action. If, in revealing the vulnerability, the person making the report has committed a punishable act, the responsible reporting of the vulnerability does not in any way safeguard him against the possibility that the police, on the authority of the OM, will instigate a criminal investigation, and/or that legal proceedings may ensue. In this letter a number of principles are outlined which the public prosecutor needs to consider when assessing the question whether legal proceedings ought to be instituted against the hacker/informant of a vulnerability or not.

In the Penal Code, the concept of hacking 'ethically' does not occur in the provisions which regulate computer piracy. The law also does not provide a specific defence for a hacker who is acting out of ideological or ethical motives. Although the law does not provide for it, this does not mean that 'ethical' motives cannot play any role in assessing the criminality of the perpetrator's action. If a hacker finds a leak in the security of an information system of an enterprise and reports this to the relevant organisation, then this is called - in principle - conscientious or 'ethical' hacking. In principle, no criminal investigation would be instituted if there is a question of restitution between the person making the report and the enterprise concerned. However, if a hacker reports a leak, but there are indications that the hacker consciously or unconsciously has done more than just report the security leak to the relevant enterprise, then that certainly needs to be thoroughly investigated. Consider such things as the copying of sensitive (personal) details or the planting of 'malware' in the system. The testing criteria that are applicable here are similar to the situations where criminal actions are committed

by journalists for the purpose of news gathering. I shall deal later with these testing criteria.

The guide in principle regulates nothing more or less than how one should preferably act when information is acquired about vulnerability in an ICT-system. The manner in which this information is obtained in itself has no bearing on Responsible Disclosure (RD). The objective of RD is the contribution it makes to increasing the security of ICT systems by reporting (possible) vulnerabilities in a responsible manner, and in dealing meticulously with these reports, so that any damage can be prevented or limited as much as possible.

That is why RD is not a 'given' of 'policy' to which anyone can appeal without further ado. Nor is RD uniform. RD is involved when the enterprise that has been hacked into also has a RD policy. If there is no such policy, there is no RD either. Naturally, when assessing the case it is possible to look at the general principles which are employed in RD and which have been described in the Guide. Further (criminal) investigation is often necessary to discover whether a reporting by a hacker was necessary and proportional under the given circumstances. If a hacker communicates directly and safely with the owner of the ICT system about a leak encountered in the security, and no data have been removed or manipulated, there can be a question of RD and there is no reason to instigate any (further) criminal investigation or any legal proceedings. On the other hand, where data have been removed, manipulated or copied, or where unauthorized access has been given to the ICT -system, there is no question of RD and further criminal investigation and possible criminal legal proceedings are indicated.

In short: in assessing whether there is question of criminal behaviour the public prosecutor will have to take account of the following circumstances:

- Was the action of the suspect necessary within a democratic society (was there an overriding public interest)?
- In his actions has the suspect acted proportionally (was the chosen means proportionate to reaching the objective)? In other words: how did the hacker obtain access to the ICT system? If access was obtained in a disproportionate manner, for example, as described in the Guide (page 8 under 4.2.), there is no question of an 'ethical' hacking.
- Has the suspect acted in an alternative manner (were there other ways to act)? In other words: was the hacking reported directly to the owner of the ICT-system or did the hacker not do this immediately in order to delete traces, to manipulate, copy or remove data? If traces have been deleted or if data have been manipulated, copied or removed, there is no question of ethical hacking.

If the answer to the above questions is positive, the public prosecutor can decide not to instigate a criminal investigation or to institute legal proceedings.

As already noted above, it may be necessary first to instigate a criminal investigation and to regard the hacker as a suspect in order to be able to obtain an answer to the above questions. In case of doubt, the case officer can consult the cybercrime officer in his/her district and/or the Knowledge and Expertise Cybercrime Centre at the National Office. It is recommended that the considerations with regard to the framework described above be, at least, recorded in a log so that the decision to prosecute can be explained at the court hearing.

Should you, as a result of this letter, still have any questions and/or remarks you can contact the Policy and Strategy Department of the Prosecutor General.

I trust that I have informed you sufficiently for the time being.

Kind regards,
The Board of Procurators General

H.J. Bolhaar