antiSecurity

save a bug, save a life

Contact us with email:
anti@security.is

Texts

Texts Index

~~~
~ Anti security "policy" v0.9 by anonymous
~ - Save the bugs!
~
~~~

-- This is my view and it does not fully speak for all the people
-- that are involved in anti security and it is subject to heavy change.

Content:

Introduction.
What is this policy?
Purpose of the policy.
Is this a joke ?
The policy.
Using the policy.
Contribute to the policy.
Thanks & reference.

[Introduction]

Hello.

This policy is designed to try to advocate a new a completly different policy for the underground community that is designed for "anti disclosure" basicly the opposite of full disclosure but with a few side notes that advocate some disclosure of bug information but in general this is designed to be a policy that people will read and think, "Hey.. this is the right thing!", hopefully.

[What is this policy]

This policy is basicly a guideline.

It will demonstrate that it is not good to post bug/exploit information to places like BUGTRAQ, packetstorm, other public forums. It will show that most of the people that are excessively posting bugs to these public forums are actually not doing it for security but quite the contrary for things like fame, jobs, etc.

The policy will show you that if you are really interested in security that there is a much better way of increasing security, because basicly when you send a new bug and an exploit to a place like BUGTRAQ you are actually decreasing security and potentially causing hundreds of thousands of people high damage from when script kiddies use your bug/exploit to break into their system.

It will demonstrate the best way to maintain the anti security policy which is to keep bugs/exploits private within either a very small group of trusted people that have the skill to understand what it is about or just simply keep it for yourself. If however the exploit leaks you should contact vendor and tell him about the bug. If the bug is discovered by someone else or the vendor has fixed the problem you are free to post the exploit to a non public forum, maybe your website.

Also it is essential to demonstrate that a person that is looking for security bugs does so just for the sheer enjoyment and thrill, difficulty of finding and obvious bug or a very difficult to find bug and then possible exploiting it, after this has taken place he should carry on and start looking for other bugs, ie: by auditing src code, doing protocol 'checks', reverse engineering and using security logic. This is an important thing in this policy that needs to be addressed. We do this because we love it!

[Purpose of the policy]

The purpose of this policy is to raise public awareness of a new way of thinking in the security scene, it is written to try to help out the anti security movement and to show interested people the best way to be a part of the anti security movement, by using this policy.

One of the main reasons for this policy and what it is meant to address is the need for none-disclosure, which is basicly because way too much stuff is getting sent to BUGTRAQ and people like us really dont like it that way and we hope that you wont like it either after studying anti security.

The purpose of this policy is to give people that are hackers a policy that they can use to keep things private as they should remain and not tempted by the dark side.

[Is this a joke?]

For some reason a lot of people think this is a joke, I've been asked about 4 times wether this whole anti security thing is a joke. And to answer your question about this policy, No! It is not a joke we take this seriously but we welcome any flames, comments or whatever that anyone might have.

[The policy]

The policy in a nutshell.

1. Do not tell the world about security bugs you find.
2. Do not release exploits to public forums.
3. If you are serious about security, notify only vendor.
4. If exploit leaks, notify vendor.
5. If bug becomes public, you are safe to release exploit to a none public forum.
6. Never ever give bug or exploit information out on a bug/exploit trusted to you by the discoverer/author of the bug/exploit. This is basis for trust, do not give what you did not write!

This will demonstrate basicly the steps and scenarios that might happen and how the policy is used in those steps, thus describing the policy.

note: fiction ;>

Okay let's create a few variables.

HACKER = The person that wants to use the anti security policy
VENDOR = Company or group that wrote the program that HACKER found bug in
COMMUNITY = BUGTRAQ, PACKETSTORM, and the like.

Background:

HACKER is an avid auditer and finds a bug in bind-8.2.2-P7 a 1 byte overflow which is pretty difficult to exploit but he manages, he writes an exploit for this bug and he gives it to a very small amount of people, possible people that are maybe in his group or that he trusts explicitly.

< scenario 1 >

HACKER who is a follower of the anti security policy does not notify the community or the vendor and the bug lives on for many years, hopefully ;> Causing little or no damage at all.

< scenario 2 >

HACKER is a TRUE security minded person, ie: someone that really cares about security and is not the typical "hey I say I care about security but what I really want is fame and a job". Allright this person who also has hopefully read something about the anti security movement and since he really apreciates security he should ONLY contact the vendor and let them handle it.

< scenario 3 >

HACKER is a glory/fame seeker and he decides to post the bug to the COMMUNITY. Ofcorse he says it is in the interest of full disclosure and not fame and the like. He has read some full disclosure policy and notifies vendor maybe 5 days before he releases the bug and most likely the exploit too.

After the five days have passed, we must conclude that the vendor has issued some sort of hotfix or a patch to fix the security problem and now the HACKER sends the bug information, the exploit to the COMMUNITY and possible a patch too.

Now has security been increased? Do you really think that most of COMMUNITY. ie: the people that read BUGTRAQ want to patch their servers? No! It is script kiddies that are waiting for the latest warez, as soon as HACKER releases this new bug to the COMMUNITY thousands of script kiddies with little or no skill will start breaking into hundreds of thousands of boxes and if this bug were genuine, they would! And belive me lots of boxes would get destroyed.

Now, I ask.. is this a good thing you are doing by posting to the COMMUNITY all logic says NO!

< scenario 4 >

HACKER in this scenarion followed the anti security movement.

HACKER has had the exploit for a year or more and now for some strange reason you hear rumors that script kiddies have the exploit. If these rumors turn out to be correct you have an obligation to notify the vendor, so that they can issue a patch, because this can cause just as much havoc as when people post to the COMMUNITY

Q: Well what is the damn difference then?!? It is bound to leak someday.
A: Yes it happens much to often but there is alot of stuff out there that has not leaked and the best way to not make things leak is too not give to anyone at all. This however is not possible for some so the best thing is to limit it to ONLY people that you trust 100 %. And we hope that people that follow the anti security trend will also realize a crucial point which is not to give what u didn't write!

Someone else has found the bug that HACKER found and has notified the COMMUNITY and VENDOR. After this has happened HACKER is free to publish his code on a non-public forum, like his personal website. This however is not required at all.

[Using the policy]

Follow the guidelines that were outlined in previous sections, and remember what keynotes.

[Contribute to the policy]

This policy is considered pre-beta and is subject to heavy change. We need alot of help in adjusting this policy and so if you have any ideas about things that are not clear and how to clear them up then please send us that information. Also if you have things you would like to add/tweak just send it.

[Thanks and reference]

This policy is written by anonymous and it will remain that way because it is not supposed to portrait the views on a single person but of all the people that follow this movement.

However certain groups and people deserve credit:

silent for starting anti security and doing most of the work.
jimjones for writing the great intro and FAQ!
RFP for writing a policy for the full disclosure people.
Everyone that has contributed so far!

-- anonymous