INDUSTRY EVENTS

AUGUST 15, 2014 **- THU T.**

Black Hat 2014 Keynote: Cybersecurity as Realpolitik

Black Hat USA 2014 kicked off with a dense keynote from Dan Geer, the CISO of In-Q-Tel, a not-for-profit investment firm supporting the Central Intelligence Agency. However, he noted that his talk was representing his own opinions, not speaking on behalf of any organization.

With a long history of contributing to the information security industry, Dan Geer is known for his deep security philosophy and involvement in shaping security policy. Read more about his achievements in his full biography on the Black Hat website. And, the full text of his speech, should you want to read it (hey I did), is available online as well.

His speech at Black Hat, *Cybersecurity as Realpolitik*, opened with acknowledgement of the sheer pervasiveness of cybersecurity across every industry and area of our lives -

> “Not only has cybersecurity reached the highest levels of attention, it has spread into nearly every corner. If area is the product of height and width, then the footprint of cybersecurity has surpassed the grasp of any one of us.

Similarly, he makes the point that knowing how a security technology works is the only way to ensure its effectiveness; acknowledging the security industry's inherent skeptical nature:

> "It's magic!" is not the answer a security person will ever accept. By and large, I can tell *what* something is good for once I know *how* it works.

Dan then outlined 10 security policy proposals to regulate and improve upon the information security industry, including:

###1. Mandatory reporting Using the Centers for Disease Control (CDC) as an example, he pointed out their practice of mandatory reporting of communicable diseases, likening it to the need to report new discoveries of malware and cybersecurity failures.

Referencing our need to enforce protection of the public health of the Internet, Dan asks the question:

> Should you face criminal charges if you fail to make such a report [about known cybersecurity failures or breaches]?"

According to U.S. Code, it is a crime to fail to report a felony of which you have knowledge.

However, this proposal isn't as clear-cut a case as the disease analogy suggests - the differences lie in the fact that malware is still treated by amateurs; spreads globally from initiation; and is distributed by known opponents.

###2. Net neutrality

> The question remains, is the Internet a telecommunications service or an information service?

He proposes two ways about it for ISPs:

1. Charge whatever you like based on the information carried, but be responsible for the content if it's hurtful.
2. Enjoy common carrier protections at all times, but you are barred from inspecting and acting on the information carried - and you can only charge for carriage itself.

###3. Source code liability He compares source code liability to the legal concept of product liability - claiming that: If you make money selling something, then you better do it well, or you will be held responsible for the trouble it causes.

Within this policy, he lists a few guidelines to follow, including:

- **Consult criminal code to determine if damage was due to intent.** Figuring out why something went wrong and if intentional damage was the culprit is the first step - unintentional damage may be attributed to sloppy code, poor testing, incompetence, etc.
- **Deliver software with buildable source code and a license to disable any code or functionality in order to limit your liability to a refund.** Empowering the licensee to disable parts they don't want or trust should limit your liability in the event of damages.
- **If you don't share your code or allow disablement, then you will be held liable for whatever damage your software causes.** If you don't give licensees options, then you must live with the consequences of normal product liability much like any other manufacturer of a product - cars, blenders, hot coffee, etc.

###4. Strike back Striking back against an attacker is difficult, as true attribution of a crime proves extremely difficult. While some large enterprises can strike back effectively and globally, it's an expensive endeavor that smaller, domestic companies aren't afforded.

Dan recommends instead of striking back, that smaller companies or individuals should put their efforts toward quickly recovering from a blow.

###5. Fallbacks and resiliency He acknowledges that this topic is one too complicated and varied to be addressed in only one policy.

One way to address this could be built-in redundancy. When it comes to cryptographic algorithm failovers, a protocol should be in place that ensures a switch to a secondary, different type of cryptographic algorithm in the event the first one is compromised.

A different design could mandate remote management interfaces to embedded systems that allow you to remotely upgrade endpoints when needed. But he also highlights the security concerns that arise in that situation:

If it does have a remote management interface, the opponent of skill will focus on that and, once a break is achieved, will use those self-same management functions to ensure that not only does he retain control over the long interval but, as well, you will be unlikely to know that he is there.

Putting more emphasis on the access and authentication security of remote management interfaces that, while necessary for upgrades, also introduce problems if unauthorized access is gained.

###6. Vulnerability finding He suggests that the U.S. government 'corner the market' on vulnerability finding, that is, to pay vulnerability finders to discover and disclose and thus increase the rate of vulnerabilities found.

To that advantage, we would also have an inventory of the world's weapons, including vulnerabilities reported to software vendors. However, the growing number of web applications that appear to be written by machines suggest that vulnerabilities, too, will be written by machines, further complicating the vulnerability finding process.

###7. Right to Be Forgotten

> Your digital exhaust is unique hence it identifies. Pooling everyone's digital exhaust also characterizes how you differ from normal.

Dan argues that the EU's Right to Be Forgotten law is appropriate and advantageous, and that similarly, we should at least have the right to misrepresent ourselves if we choose to. He compares it to leaving town or changing your name.

Similarly, those that help the government are granted the 'right to be forgotten' via witness protection programs. Why shouldn't the same liberties be granted to all?

###8. Internet voting He remarks on the compromise of election integrity that would be introduced by online voting, supporting NIST and the National Center for Policy Analysis in their discouragement of the idea.

###9. Abandonment What counts as abandonment? Dan argues that any product that no longer receives security updates counts as abandoned.

He also suggests a policy that mandates any abandoned code base must be open-sourced.

###10. Convergence This refers to the merging of the physical and cyber worlds, and what happens as a result, as summed up by a few points made by the Pew Research Center:

1. Nation-states attempting to maintain security and political control will lead to more blocking, filtering, segmentation and balkanization of the Internet.
2. News of government and corporate surveillance evokes more mistrust.
3. Commercial pressures will endanger the open structure of online life.
4. Over-compensating efforts to mitigate the "too much information" problem may thwart content-sharing.

He concludes with a great quote about the title:

> Realpolitik means, in the words of British historian E. H. Carr, that what is successful is right and what is unsuccessful is wrong, that there is no moral dimension in how the world is, and that attempting to govern based on principles cannot succeed. Realpolitik is at once atheistic and anti-utopian.

And when paired with cybersecurity:

> Realpolitik says that what cybersecurity works is right and what cybersecurity does not work is wrong and Realpolitik thus resonates with Howard's "Security will always be exactly as bad as it can possibly be while allowing everything to still function."

At the end of the day, policies that reflect reality in terms of what works and doesn't, is all that will be effective in cybersecurity; not policies based on principles - which he states here:

> In the end, reality always wins, and the reality of technical facts has more staying power than the reality of market share or utopian enthusiasm.

By and large the most philosophical security speech I've ever witnessed, Dan's eloquent metaphors introduced a very different side of infosec, one not mired in details and technicality, but solid facts and forward-thinking hopes for shaping and improving security policy.

Tags

Blackhat

Authors

THU T.

Product Marketing Manager

@Thu_Duo

Related

INDUSTRY EVENTS

(Vis a) Viva Las Vegas: Catching Up With Duo at Black Hat 2018!

INDUSTRY EVENTS

The Best Beards of Black Hat (and DEF CON)

DUO LABS

A Place to Hang Our Hats: Intern Goes to Vegas