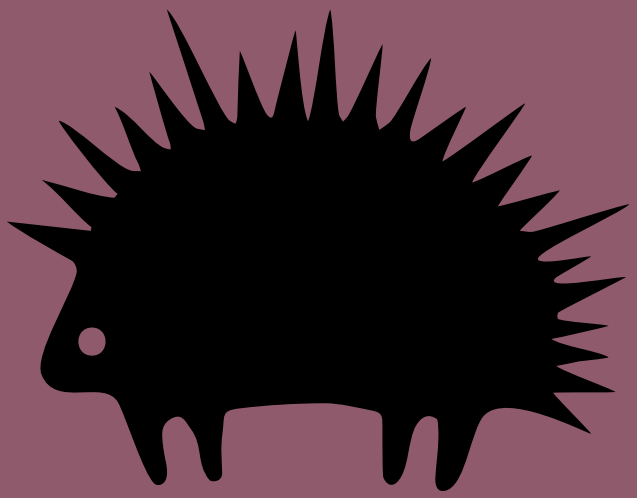
PRIVACY INTERNATIONAL

Advocacy Briefing on Thornsec

What Policymakers Can Learn About Cyber Security From Thornsec



Background

In November 2014, Privacy International went dark, to the outside world at least. In late October, Drupal revealed[1] it had discovered a major vulnerability in its services, which had likely compromised any website running on it. Drupal provides an open source content management system (CMS) used by millions of organisations worldwide to run their websites, including, at the time, Privacy International. The vulnerability was so severe, Drupal's security team advised people using their software to presume the worst: attackers could have copied all the data from the site for malicious purposes; attackers could have created a 'backdoor', enabling the attackers to access other services running on the server - all without being detected or leaving a trace.

The same day, Privacy International was about to launch a new fundraising campaign, which would have involved collecting personal information from donors. The month before, we had just launched a new website[2], one that we couldn't confidently patch. The vulnerability in the Drupal CMS meant the platform on which this personal information for our fundraising campaign was to be collected could be compromised. So Privacy International made the difficult decision to shut down the new website permanently and sacrifice the fundraising campaign. Privacy International then started a multi-year redevelopment process to rebuild the website from scratch. This process highlighted the need to examine our organisational security as a whole, particularly defending our network from attacks and data loss.

1 Drupal PSA-2014-003, available at https://www.drupal.org/forum/newsletters/security-public-service-announcements/2014-10-29/drupal-core-highly-critical.

2 Privacy International website circa 2014, available at http://web.archive.org/web/20141004124430/https://.www.privacyinternational.org/

What is Thornsec?

Thornsec is a piece of software developed by Privacy International's Tech Team which is an automated way to deploy, test, and audit internal and external services for an organisation, saving a lot of time and creating a sustainable security model. We are using this software to run all of Privacy International's services – website, calendar, project management tools, Tor hidden services, VPNs. The whole system runs on two servers and the whole cost is around US$1000 to set up. The "Thorn" is a reminder that the software is designed to be a thorn in the side of adversaries who may want to access or damage our network, and therefore frustrate attempts to breach our "sec", or security.

But this briefing is not so much about the technology. Nor is Thornsec solely a technological initiative, it is also changing the culture of the organisation by making us all pay more attention to the technology we take for granted every day. It places responsibility for security where it belongs: the executive leadership of the organisation. It also engages with every individual on organisational security.

Through tearing apart our services and rebuilding our organisational network we have learned much. The most important lesson, learned through a combination of frustration and wonder, is that it is both necessary and possible to increase security understanding across an organisation. And that is a strong basis for good cyber security policy more broadly. Our aim in this briefing is to share how developing and implementing Thornsec is influencing our policy work, and how it could help you too.

Why do we need Thornsec?

Security is hard. Even multi-million dollar organisations and security and critical infrastructure departments of governments get it wrong. This is evident in the continuing global data breaches- from poorly secured databases in company networks to ransomware spreading with relative ease through networks. So how could we, a small NGO with limited resources, be better at securing our networks and reduce the risk of hacks, phishing, ransomware and data breaches, which plague so many organisations?

As an NGO we face challenges in the same way as any small or medium sized enterprise (SME) when it comes to technology. But tech knowledge is expensive, hard to find, and until recently was not even considered in funding models. Therefore our internal systems were often left unmaintained, unpatched and bordering on insecure. If an organisation's network is insecure, ransomware or a hack can spread through an organisation, causing untold damage, as demonstrated in the recent Wannacry and NotPetya attacks.

Why is network security important?

Privacy International believes that protecting and defending individuals, devices and networks[3] should form the basis of any cyber security strategy. Individuals, devices and networks are interlinked and interdependent. Defending security means securing all three, simultaneously. Examples of security failures across all three domains are evident in almost every major cyber-attack.

3 Privacy International, Cyber Security in the Global South, London. Available at https://privacyinternational.org/sites/default/files/Cybersecurity_2017.pdf.

How to secure networks is an integral yet often neglected part of cyber security policy discussions. If, as a society, we are to have a hope of protecting both our privacy and our security when using technology, networks must be secure by default, from the start. Good network security means reducing the attack surface and then allowing the right people through the right devices to access the right services on a network, and keeping everyone and everything else out. Protecting and defending a network can mean protecting a home Wi-Fi network, a company's intranet, a telecommunications network accessed by the public, a bank's network, an industrial control system (ICS) in a factory, or a nation's critical infrastructure, such as a power grid.

We get nervous when we hear Privacy International's Network[4] of partner organisations being advised to focus solely on the security of their devices, or end points, in order to protect their privacy and security, by using web applications like Tor and secure messaging services like Signal. This advice places responsibility on end users to secure only their devices, which ultimately leaves them vulnerable in other ways. It doesn't matter how secure or insecure the endpoints are if a network itself is insecure. So we believe it is not enough to concentrate on the end point, we need to look at organisational security and an organisation's network as a whole.

4 Privacy International Network, available at https://privacyinternational.org/privacyint-network.

5 Steps To Better Network Security:

1. Admit there is a problem.

Security is hard. The first step is to admit this and understand that the systems we rely on every day are fragile. We are building on top of existing systems we wrongly assume to be secure by default. It should be presumed that services will fail or crash at some point, and there is a high risk that data could be lost. This could be due to system failures but also physical factors: There could be a power failure or offices could flood, resulting in physical damage to computers and servers. Devices could be seized or stolen, or just lost.

When we fail, which we will, we need to fail well and that means failing safely. In the current climate, systems are failing, but they are not failing well or safely. Thornsec addresses these key issues.

Failing well means that if a system crashes or fails temporarily, an organisation is protected from data loss and does not grind to a halt. This means data is backed up, encrypted and easily retrievable so the organisation can continue to provide services under these circumstances with minimal disruption. Failing safely means that when a system crashes or stops working altogether, it is better that the system and the data held within it are destroyed altogether and rebuilt from scratch, so there is no risk of data being stored insecurely. Because encrypted backups exist, both virtually and on servers in other locations, rebooting the office to a new installation (rebuilding services from scratch) would take a day. If a service fails (crashes or dies completely) it will not be restarted until it can be audited to work out why (a bit like sending a crash report to Apple or Microsoft) and to verify there has been no breach of services (data has escaped or been lost).

2. Change the perception of cyber security by taking a community healthcare approach.

Cyber security should be considered a public good in the same way as public health, for example, which promotes collective responsibility[5] for the benefit of everyone. When the US State of Oregon passed a new cyber security law, the Chief Information Officer described it as a move to apply a "community healthcare model". He said,

"Just like a community, when one of us has measles, then everyone is going to be at risk for measles unless someone, somewhere makes sure that everyone has their inoculations up to date, and we can identify it quickly and take care of it and that we can make sure that we have the right practices in place to keep everybody else from getting infected by it.[6]"

Cyber security, like public health, involves collective efforts. We understand how germs spread in the physical world, but do we understand how different kinds of bugs spread between computers? In developing and implementing Thornsec, each of us at Privacy International have an increased understanding of how the organisation runs technically, which gives us ownership over our network and a sense of responsibility for our own devices… we even install our own root certificates. In a cyber security context, securing the individual helps secure everyone. This concept of a community healthcare approach scales, and it should be the approach taken by policy makers and regulators.

3. Make Time For Patching

Patching means regularly installing software updates for operating systems. Patches fix bugs in code that make services vulnerable to hacking. A big part of security is about patching and maintenance and this should be made as easy as possible. For a smaller organisation like Privacy International, we need to be able to patch our own services. Thornsec is designed so that this process takes no time at all.

5 Schneider, F., Sedenberg, E., Mulligan, D.: Public Cybersecurity and Rationalizing Information Sharing, Opinion Piece for the International Risk Governance Center (IRGC). Lausanne: IRGC. Available at https://www.cs.cornell.edu/fbs/publications/publicCybersecRisks.pdf.

6 Johnson, R. "Oregon advances CIO's office toward cybersecurity unification with new law, advisory council." statescoop [Oregon] 6 July 2017. Available at http://statescoop.com/oregon-advances-cios-office-toward-cybersecurity-unification-with-new-law-advisory-council.

For the devices connected to our network that can't be patched, Thornsec provides another solution, as outlined in the last two sections below.

However, as a wider policy point, in some complex networks it is just not possible to patch and this must be taken into account too. For example, in the UK, the National Health Service (NHS) was a victim of the WannaCry malware and many hospitals were affected. This attack highlighted the difficulty in patching when it comes to complex networks and expensive medical equipment. The truth is that when operating systems are embedded into expensive equipment, say an X ray machine, there is no way to patch/ update the software. Cyber security experts have shared[7] their horror stories from over the years, for example when a network worm accidentally took fetal heart monitors offline in a natal intensive care unit. To secure equipment like this takes a considerable amount of expertise, and organisations like hospitals don't always have full time cyber security experts to address these issues.

So while "patch, patch, patch" is very good advice, it must also be recognised that defensive security is hard. Some systems are more complex than others, and some devices are not designed to be patched. It is important to be aware of this when developing cyber security policy.

4. Remember that your router is not your friend.

Software updates do not just apply to devices like a laptop or phone, but also those running on a network, such as a router or a connected printer. If a device is hacked, a whole network is also at risk. For example, following a systems breach at the US Chamber of Commerce in 2011, the Chamber worked with the FBI to secure its systems. Months later, it was discovered[8] that an internet connected thermostat and printer were still communicating with computers in China.

7 Woods, B. "The NHS got lucky – for now. Cyber-attacks will only get worse." The Guardian [London] 15 May 2017. Available at https://www.theguardian.com/commentisfree/2017/may/15/nhs-cyber-attacks-ransomware-crisis.

8 Perlroth, N. "Hackers in China Attacked The Times for Last 4 Months." The New York Times [New York] 30 January 2013. Available at http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

So when was the last time you updated the software on your router, or your printer at home, or in the office? You probably will struggle, as many devices have poor security such as no or default passwords, and are difficult or even impossible for everyday users to change. This leaves devices vulnerable to being hacked, famously demonstrated in October 2016 when malware, known as Mirai, powered a huge denial of service (DDoS) attack, enabled by a botnet of hundreds of thousands of infected internet connected devices like webcams and baby monitors. The malware scanned the internet for devices protected by factory default usernames and passwords. It targeted the Dyn network that hosted a range of popular websites such as Twitter, Netflix and the New York Times, which were made inaccessible for a time.

Think about the Wi-Fi router provided by an internet service provider (ISP), which lies at the centre of any network security. It is the gateway into the home, office, factory, parliament or military base. A router provides access to all the devices that connect to it. Privacy International's technologists did not want to trust the router supplied by the ISP, for the reasons outlined above and also as the traffic coming in and out could not be controlled. So, they put another router between it and the organisation's internal services, which essentially works like a firewall and segregates traffic (see below).

Policy-makers and regulators need to address how they will encourage connected devices and product manufacturers to make devices more secure, particularly when there is currently no market incentive to do so. This will take time. In the short term, organisations should be encouraged to take steps to ensure that vulnerable devices are not risking the health of an entire network. This involves de-centralising services, as outlined below.

5. Consider centralisation an enemy of security.

Most NGOs and SMEs rely on their ISP supplied router as their wired and wireless access point. There is no segregation of traffic, and devices can 'talk' to each other, and the wider internet, unhindered. Network devices are designed to be promiscuous. They are designed to advertise they are there for all to see and connect to. For example, if you scan a network from your laptop to connect to a printer, you are essentially waiting for a printer to advertise it is there.

This constant signaling and talking create a large "attack surface". If one device is broken into, all devices on the network can be broken into as they are all talking to each other unhindered. To reduce the attack surface in Privacy International's network, Thornsec ensures internal services are protected by ensuring devices are only signaling and talking to each other when it is needed. Computers can talk to printers (to tell it to print something) but the printer can't talk back unless invited (to confirm the job is done). Each device and service is isolated. This means that if one device is compromised, it would be contained and wouldn't spread throughout the network.

The simplicity of the idea of Thornsec has made us realise what it means to be secure, and how our devices and services are betraying us. Devices and services 'talking' to each other to collect data, often unnecessary to carry out their functions, is making us vulnerable by creating a large attack surface.

Conclusion: Developing Policy With Help From Snowden and Chelsea

Companies and governments build systems, devices, networks and services that generate and accumulate vast data stores without proper regard to risk, security, or data minimisation. Because it is cheap to connect devices to the internet, every conceivable thing is being connected to the internet without regard to security. Governments' surveillance ambitions and industry's voraciousness for data, and their disregard to data security, are increasing the attack surfaces and making us all vulnerable.

This makes network security all the more important. This means ensuring that the right people through the right devices are allowed to access the right services on a network, and keeping everyone and everything else out. Developing Thornsec and stripping away everything apart from what is essential for our services to run has revealed to us the areas that we believe make good policy for network security.

These are the 5 lessons we have learned:

1. Admit there is a problem and ensure you fail well when systems crash or fail (which they will). The first question any organisation should ask itself is how it is protecting and backing up data. Is it easily retrievable, say, if the office burned down?

2. Change the perception of cyber security by taking a community healthcare approach. Cyber security should be considered a public good in the same way as public health, which promotes collective responsibility for the benefit of everyone. Increase knowledge and understanding of this concept and let people take ownership of their own security.

3. Make time for patching. Design networks so that patching takes no time, and address the areas where patching cannot take place. Don't ignore it.

4. Remember that your router is not your friend. While addressing device insecurity is a long term policy goal, work arounds should be developed in the short term.

5. Consider centralisation as an enemy of security. De-centralise services as much as possible. Separate services so if one gets hacked others won't.

While Thornsec was designed for the needs of a small organisation, the concept and principles scale – from home networks to businesses to governments to military. Thornsec is a work in progress and we are learning from it all the time. We use open source as much as we can so that anyone anywhere can adapt our software for use, and our lessons are shared openly too [link to blog series]. If there are attacks against our system we want to be able to log them to see if we can learn from and share them with others.

Nothing is 100% secure, but we are confident Thornsec is making us more secure. It is addressing a fundamental issue: the complexity of our systems is increasing, and we are building on top of existing systems we assume to be secure but they are not. Security is hard, defending networks is hard. After all, an attacker only has to succeed once, but defenders have to be safe all the time. Cyber-attacks are only going to get worse and must be urgently addressed. Shaping good and sensible cyber security policy to address these challenges demands an understanding of what it truly means to be secure. Implementing Thornsec helps with that. Take it from us, from our experiences of failure: from failing badly by killing our website, to struggling every day to fail well.

* Snowden and Chelsea are the names of our servers.