The Guardian

The state of cyber security: we're all screwed

Sophisticated cybercrime, privacy fears and ongoing confusion about security have soured the internet for many, and doing something about it won't be easy

Dan Tynan *in Las Vegas*

Mon 8 Aug 2016 15.07 EDT

When cybersecurity professionals converged in Las Vegas last week to expose vulnerabilities and swap hacking techniques at Black Hat and Defcon, a consistent theme emerged: the internet is broken, and if we don't do something soon, we risk permanent damage to our economy.

"Half of all Americans are backing away from the net due to fears regarding security and privacy," longtime tech security guru Dan Kaminsky said in his Black Hat keynote speech, citing a July 2015 study by the National Telecommunications and Information Administration. "We need to go ahead and get the internet fixed or risk losing this engine of beauty."

There's no lack of things to be worried about: organized cybercriminal gangs; government surveillance; not to mention hack attacks from nation states.

That may be good news for the cybersecurity industry, which is expected to grow more than 10% annually and surpass $200bn worldwide by 2021, according to research firm Markets and Markets.

But it's bad news for the rest of us. As we conduct more of our lives online, we're being asked to become increasingly savvy about computer security. Many are simply uninterested or not up to the task.

Add up all these factors, and the question becomes not why many consumers are losing confidence in the internet, but whether they should have any confidence at all.

Consumers: the new ATM for cyber crooks

The online crooks' weapon of choice: crypto-ransomware, which encrypts all the data files on a user's machine, making them inaccessible. The malware, which accounts for nearly 60% of all infections, according to research firm Malwarebytes, then displays a screen demanding hundreds of dollars. If victims don't pay up in time, the files are destroyed.

"Over the last few years attackers realized that instead of going through these elaborate hacks - phishing for passwords, breaking into accounts, stealing information, and then selling the data on the internet's black market for pennies per record - they could simply target individuals and businesses and treat them like an ATM," says Brian Beyer, CEO and founder of enterprise security firm Red Canary.

According to Symantec, the average ransom paid doubled from just under $300 in 2015 to $679 this year. Last year, the criminals behind the CryptoWall3 malware cost victims more than $325m, according to estimates from the Cyber Threat Alliance; 2016's haul is expected to be significantly higher.

Dan Kaminsky speaks during his keynote address at the Black Hat cyber security conference in Las Vegas: 'We need to go ahead and get the internet fixed or risk losing this engine of beauty.' Photograph: David Becker/Reuters

A ransomware attack is relatively easy to overcome if you have a current and complete copy of your data; you can simply restore the untainted files to your machine, says Beyer. (Before you do, though, be sure to install security software that will remove the ransomware, or you may find yourself being jacked all over again, he warns.)

The problem? About 3 in 10 people never back up their data, while others do it sporadically. And even for those who do backup religiously - or use software such as iCloud or CrashPlan that

automatically copies files to machines in the cloud – restoring data can be a hassle.

Which is why for many victims it just seems easier to pay up, says Beyer. And that's what the criminals are counting on.

The cyber enemy is us

It's a truism that the biggest threat to security isn't increasingly sophisticated cyber criminals, data-hungry corporations or even espionage-happy nation states; it's the people who get duped into clicking random links or opening rogue files.

To paraphrase Pogo: we have met the cyber enemy, and he is us.

In a Black Hat demonstration, Zinaida Benenson, a researcher at University of Erlangen-Nuremberg in Germany, measured how many people would click on a potentially malicious link inside an email, then compared the results to how many did the same with a message they received on Facebook. (Spear phishing, or targeting a specific person via a message containing bogus links, is a common way for attackers to steal information.)

The results: one in five test subjects clicked a link from a stranger in an email; more than twice as many did it on the social network. Lured by curiosity, even tech-savvy users in the study could not resist clicking.

In another study, Elie Bursztein, head of Google's anti-abuse research team, tracked whether people would pick up a USB thumb drive they found lying on the ground and stick it into their computers (which, he noted, was used as a major plot point in season one of USA Network's Mr Robot). His research team left 300 USB drives at various locations at the University of Illinois Urbana-Champagne campus. Unwitting test subjects picked up 98% of them; nearly half plugged the drives in and opened the files contained on them.

Ask security companies what consumers should do to stay safe, and you'll get the same advice they've been handing out for years – use better passwords, keep software up to date, back up your data, etc. Dan Kaminsky's advice is more stark: keep a close watch on your financials and immediately report anything that looks suspicious.

"If you have a bank account that will not send you a text message when there's a transaction, move your money," he says. "Because now it's not about preventing the fraud, it's about seeing it as soon as it happens."

In other words, assume you're going to be hacked, and try to catch it before it does too much damage.

Could the situation change?

If everyone really followed all the advice out there, we wouldn't be in this mess. But they don't. Many consumers will never do any of these things, and scant few will do all of them all the time.

Jake Braun, CEO of strategic security consultancy Cambridge Global Advisors, says moves by companies such as Apple, Google, and Facebook to encrypt data and communications are a huge step in the right direction. When your data is encrypted, the bad guys can't get to it. (And, sometimes, neither can the good guys. That's why the US government is putting huge pressure on

these companies to relax their encryption standards to allow access by law enforcement - known colloquially as "the crypto wars".)

Braun is optimistic that as younger generations take over, they'll demand more secure versions of products from vendors. Still, he says, the scope of the problem is so large that more government intervention is needed.

"I think consumers should be putting more pressure on their elected officials to fund criminal investigation programs that more aggressively track down cyber criminals domestically and abroad," Braun says. "For example, the Homeland Security investigations unit investigates many types of cybercrime (most notably child pornography and online human trafficking that often targets unwitting children) but is embarrassingly underfunded."

In his keynote, Kaminsky called for a federal agency devoted to security issues, similar to the National Institutes of Health, that can "create engineering solutions to the real-world security problems that we have".

"It can't just be two guys," he said. "I need a pile of nerds to be able to work for on this 10 years. We can support health and energy and roads and cars, but somehow we can't support the thing that is driving our economy right now? That's crazy."

Topics

Hacking