If security breaches are the problem, encryption is the answer

By Neil Cosser

5 May 2016

Encryption has this kind of reputation that it's complicated. It's not. It's very, very simple. There should be no reason why an organisation shouldn't be encrypting its data in 2016.

Neil Cosser

The technology is there. And the rationale for using it is simple: breach prevention is dead. Our 2015 Breach Level Index showed over 1,600 disclosed breaches worldwide. That led to more than 700 million records being exposed. To put it simply, blocking breaches isn't working.

As we watch hackers hone in on data critical to our lives and our businesses, we need to develop a mindset that accepts attackers will find a way in - but that our critical data is protected so it doesn't make its way out.

Attackers pursued and achieved more valuable and durable information in 2015, according to the same Breach Level Index. While bad guys pilfered less financial data, the main takeaway from the report was the focus on long-lasting information (think of your health records or massive, comprehensive government databases) that allows them to conduct other attacks.

Hackers, in short, understand that it's way harder (or even impossible) to change your ID number than it is to cancel a credit card.

Enduring value of data

Bad guys see the enduring value of this data. At a consumer level, if a hacker can capture key information on an individual, they can potentially attack not only that individual but the organisation they work for and other organisations that the compromised person accesses online. Compare that to what happens when a digital attacker steals your credit card information: if the credit card's compromised, it's comparatively easy for that credit card to be rejected, stopped, and a new credit card issued.

Turning to corporations, you don't need to think data science is the sexiest job of the 21st century to see how companies are putting data at the heart of their business decision making like never before.

So where will clever digital attackers attack? At the integrity of key business data. If a key driver of whether a company manufactures more or less widgets is its big data analytical approach, a nefarious digital intruder might just tweak the data, altering its integrity in a way that the organisation would be unable, at first glance, to notice. Such attacks don't need to steal a single bit of information to make a dent in a competitor.

Painful recovery

The company, unaware of the faulty basis of their decision making, continues to drive its business ahead, making a slew of decisions downstream from the breach that are all faulty because of tampering with the original data. Companies could go months on broken assumptions and off-base approaches - making recovery from such an attack that much more painful to ameliorate, costly to the bottom line, and impactful on a company's reputation.

To consider how hard it is to prevent an attacker from ever getting into your network, think about the hyper connectivity of the near future manifest in the Internet of Things (IoT).

Even one digitally-connected gadget has at least five different parties touching the data it generates: the manufacturer, the consumer, the cloud provider hosting that data, the smartphone maker on whose phone the consumer runs the app that controls the gadget, and at least (usually) one other gadget that digitally connects to our first IoT device. And when our homes or our cars are chock full of connectivity, the number of connections is going to be a lot greater than five.

©weerapat kiatdumrong via 123RF

Faulty defence

At any point in that transmission chain, a hacker could breach a faulty defence and start siphoning off our key information. If any one part of that sprawling web of connectivity gets compromised, we have a problem.

It's not hard to see why securing this intricate web of connections is an awe-inspiring task, even for the most sophisticated technologists. Now consider a massive enterprise with thousands of devices, a mobile workforce carrying those devices across the world, and digital attackers using increasingly sophisticated approaches to find the smallest crack in our collective digital armour.

Which brings us to a crossroads. We can stick our heads in the sand and believe that a breach isn't going to happen to us because of our superior prevention or that our data isn't valuable enough to matter.

Given the more than 1,600 breaches in 2015 worldwide, this seems, shall we say, unwise. Alternatively, we can focus on protecting the asset that hackers are really after: data. Which brings us back to not only encryption but a mindset that takes breaches as a given and focuses instead on protecting data.

Reputational damage

Security leaders at organisations large and small need to admit that they are going to be breached - and then figure out what to do from there. What data is going to cause them massive reputational damage? What data, in the event its integrity is compromised, is going to kill their business?

By making the shift from considering more extravagant (and expensive) ways to keep bad guys out to protecting core assets once a diligent hacker eventually gets in, information security leaders will begin thinking in a totally different way. They'll begin to evaluate risk better and apply core information security controls, encryption, key management, and authentication.

It sounds oxymoronic, but this type of approach leads to what we call a 'secure breach'. Even when the attacker breaks through, the locked box they find inside is way less useful than the sprawling flows of data they unlocked in the unencrypted past. And, while encryption is one of the most obvious strategies for preparing for a breach, only 48 of the data breaches in 2015 - less than 4% of all breaches - involved data that was encrypted to any degree.

We've got to accept the fact that breaches are going to happen. And to keep them secure, the answer is encryption.

ABOUT THE AUTHOR

Neil Cosser, Identity and Data Protection Manager for Africa at Gemalto