


Securing the network

By Rachel Cochran
Kirk Nesbit
Dan Ourada

Simple Truths

Brian Krebs' January 17 post on Krebs on Security, "DNI: Putin Led Cyber, Propaganda Effort to Elect Trump, Denigrate Clinton," is not only an excellent piece of analysis, it also contains important cybersecurity lessons. In the post, Krebs lists five "fairly simple, immutable truths" that should strike fear in anyone interested in merchant security:

- If you connect it to the Internet, someone will try to hack it.
- If what you put on the Internet has value, someone will invest time Even if what is stolen does not have immediate value to the thief, he can easily find buyers for it.
- The price he secures for it will almost certainly be a tiny slice of its true worth to the victim.
- Organizations and individuals unwilling to spend a small fraction of what those assets are worth to secure them against cybercrooks can expect to eventually be relieved of said assets.
- These "simple truths" resonate loudly as the conversation about merchant security continues. EMV, point-to-point encryption and tokenization are not sufficient defenses from cyber criminals. The merchant environment still contains valuable data — and the immutable truths still apply.

Breaches

Attackers use any number of strategies to steal data and the consequences of a data breach can be far reaching. Some of the more prominent recent data breaches include the following:

1. Mirai botnet. In October 2016, attackers leveraged connected Internet of Things (IoT) devices to launch a DDoS (distributed denial of service) attack against Dyn (an Internet infrastructure company). No data were stolen and no payment data were breached, but even without a compromise of the merchant environment, merchants likely suffered. The attack caused instances of "clogged pipes," which created intermittent issues accessing the Internet, preventing merchants from processing payments or accessing cloud-based services and degrading the consumer experience. The attack was made possible because devices had been connected to the Internet without changing the default login.

2. Yahoo! Yahoo! reported in late 2016 that it had been the victim of two major data breaches in 2013 and 2014 that affected over one billion user accounts, the largest breach ever discovered. The Yahoo! network itself was breached, and names, email addresses, telephone numbers, dates of birth, and other user data were compromised. One major repercussion of this breach: According to Tech Times, Verizon is rethinking its bid to acquire Yahoo! assets or may significantly reduce lower its $4.8 billion bid.

3. Wendy's. In January 2016, Wendy's reported that malicious software had been discovered on POS systems in approximately 300 locations. In June, Wendy's issued a separate statement providing information that the affected locations were "considerably higher than the 300 restaurants already implicated." The path to the card data in this case? Compromised service provider's remote access credentials. The number of credit cards compromised was not provided.

4. Hollywood Presbyterian Medical Center. The Center paid $17,000 in ransom in February 2016 after hackers penetrated their systems and locked staff out of certain devices. Ransomware attacks are on the rise and while it appears that data are typically not "stolen," there are business losses and customer service impacts.

Value

When determining value of a breach, the typical components are: fines, the cost of repairing the cause of the compromise, lost business, reputational damage, etc. But it is also important to consider the value proposition for the attacker. Understanding an attacker's motivation can help in the creation of a holistic data security plan and prioritization.

Examples of data value from “The Hidden Data Economy” report from McAffee in October 2015.

PrimaryAcct, CVV, ExpDate	$5-10 US, $25-30 in EU per record
AnnotatedCC data: address, PIN, SSN, DOB	$30 US, $45 in EU per record
Bank credentials with $2,200 balance	$190 per record
Bank credentials with $6,000 balance	$500 per record
Online content services	$0.55 – comic book site $7.50 – cable streaming $15.00 – professional sports streaming

The obvious place to start is in securing payment data, but what if you already have EMV, end-to-end encryption, and tokenization in place? The next place to look is card not present (CNP) transactions. As the technologies above are introduced, attackers are transitioning to online attacks.

Securing the Network
The following steps are not exhaustive, but — in addition to securing payment data — they are essential elements of any small-business data security plan.

- **Keep applications, Operating Systems and firmware updated.** Many attacks target vulnerabilities for which a vendor has already released patches. Sign up for notifications of vendor updates for all products in use and install those updates in a timely fashion.

- **Implement a firewall.** Use a firewall to restrict what traffic can enter and leave a customer’s environments, reducing an attacker’s ability to gain access. A firewall also mitigates one of the major issues presented by IoT devices: Some vendors stop supplying security patches to devices long before the device would be expected to be removed from the environment, creating vulnerability. Don’t allow internet access to IoT devices unless absolutely necessary; if such access is essential, secure the device as thoroughly as possible.

- **Change default credentials.** Default credentials on applications and devices such as routers, firewalls, wireless access points, etc., are readily available and attackers frequently use them to gain access to systems. Always change default credentials — not only the password, but also the account name if possible — and make the password complex.

- **Do not share credentials between systems.** Brushing off news of credential compromises because nothing sensitive was compromised is a mistake. Attackers know people reuse passwords across sites and systems and will try stolen credential information against more valuable targets.

- **Back up your data.** Implement a backup routine that protects customers data against system failures, accidents and ransomware. Ensure that backups themselves are not vulnerable to ransomware; if you keep backups on a general-use file server, a successful ransomware attack will lock them along with everything else. Even a willingness to pay the ransom may not mean data will be recovered; some victims of ransomware attacks who have paid hackers have never recovered their data.

The Road Ahead

In a chaotic world where breaches are constant, it is difficult to remain optimistic. The simple, immutable truths do not help, but playing ostrich is also futile. We are all in this struggle together. Keep your heads up, engage in the security dialog, follow the advice given here, print out the simple immutable truths and tape them to your mirror. Help your customers secure the network!

Rachel Cochran is a Sr. Leader of Application Security at Vantiv
Kirk Nesbit is Vice President of Design and Support Services at SYNNEX Corporation
Dan Ourada, of Vantiv, is a Technology Evangelist