HARDENED MULTI-FACTOR AUTHENTICATION INCREASES ENTERPRISE PC SECURITY

INSTEAD OF A SECURITY PROBLEM, ENDPOINTS BECOME PART OF THE SECURITY SOLUTION

SUMMARY

The internet and mobility have made enterprise security monumentally more difficult. Employees can take mobile devices with them everywhere they go, but these smartphones, tablets, and notebooks vary wildly in terms of security features to prevent unauthorized access. Increasing numbers of endpoints became convenient targets of hackers looking to gain access to enterprise data. Many major hacks in the last few years targeted user endpoints, and the scope and pace of these attacks is growing. **Hardened multi-factor authentication (MFA)** is becoming a requirement to protect these users and the endpoints they control from attacks using stolen credentials. Intel's newly-announced Authenticate supports hardened multi-factor authentication.

RECENT ENDPOINT HACKS HAVE UNPRECEDENTED CONSEQUENCES

Many publicized hacks of major companies occurred in the past few years. Two Sony divisions were hacked, Sony Network Entertainment and Sony Pictures, with over 77 million customers affected.[1] Hacks in 2015 include Experian, which affected 15 million T-Mobile customers;[2] Ashley Madison, with 37 million accounts; and the US Federal OPM, which affected 22 million government workers. These breaches look small compared to Anthem's, where thieves stole the data of 80 million customers and another 19 million potential customers. In the last few years, breaches increased in both frequency and size, with 2014 and 2015 being especially active years.

In many recent hacks, endpoints were targeted as the weak points of a corporate network. Some were executed with social engineering, a method of social coercion, or a combination of social engineering with physical access to endpoints. Sometimes the endpoints were computers used by employees of the company. In the Target hack that shook the company in 2014, it was a 3rd party HVAC company.[3] While the exact details still have not been revealed, it is likely one of their endpoints or network connections were compromised.[4] Hackers installed data-capturing software in many Target stores nationwide and stole some 40 million credit card numbers from customers.

In the past, companies notified users about a hack, offered credit monitoring services to customers, and a few low level people lost their jobs.[5] All that changed after the Target hack. As a result of the data breach, over 90 lawsuits were filed, and the company eventually settled: $10M for customers and $39M to financial institutions. In total, Target spent $290M related to the breach and expects insurers to reimburse them for $90M of that, leaving $200M the final cost of the hack.[6] After 35 years with the company Target's CEO also resigned,[7] and the board replaced their CIO, demonstrating that employees at all levels are going to be held accountable for these hacks. CIOs as well as CEOs must take security more seriously than ever before if they want to keep their jobs.

Trends in Security & How to Combat New Threats

With more millennials in the workplace and changing working patterns, more employees use enterprise PCs outside the physical office,[8] making company data even more vulnerable. Additionally, older PCs running older operating systems with dated authentication hardware are not as secure as newer OSs like Windows 10 and lack hardware-based and OS-level security.

Passwords alone were never a secure form of authentication, but the industry historically did not have many answers to fix the issues with them. Some companies used two-factor authentication with smart cards, particularly those with top secret information. But the majority of enterprises used single authentication and single sign-on (SSO), which gave a user access to the enterprise with a single password. Because passwords alone are not secure enough, some companies are moving towards biometric forms of authentication in addition to user PINs or passwords, including fingerprint, iris scan, voice recognition, or a full face scan. These hardware methods of authentication are beginning to gain traction as alternatives to passwords.

As a result of the theft of millions of users' data, some companies have begun to employ **multi-factor authentication** (MFA) as standard operating procedure. MFA schemes have existed for quite a while, but with the advent of smartphones, more companies are using smartphones as a hard token or second factor of authentication through SMS messages. However, this type of MFA can be arduous to a user.

Windows 10 Helps Make Enterprise PCs More Secure

Technologies like 3D cameras, fingerprint sensors, microphones, and iris scanners were enabled for biometric authentication in the past, but these technologies were

generally expensive, hard to implement, and hard to use. However, the latest generations of these technologies are both inexpensive to implement and easy to use when authenticating with a PC. What also makes these technologies easier to use is native Windows 10 support as authentication methods, which makes the process much smoother and improves the user experience overall.

Many users make mistakes when typing passwords or forget them entirely. With a 3D camera, there is no forgetting, since the camera is designed to recognize a user's face and log them in without a password. This authentication reduces friction when a user moves between endpoints and allows the security regime to continually check that the user in front of the endpoint is indeed the authorized user. Thanks to new operating systems like Windows 10, these kinds of smooth user experiences are possible.

Microsoft says Windows 10 is their most secure operating system, and much of its security relates to native support for multi-factor authentication. Up until this point, most forms of multi-factor authentication were not natively supported. In Windows 10, the OS itself supports hardware like 3D cameras, fingerprint sensors, iris scanners, and smartphone-based tokens. This added level of security is critical for enterprises trying to ensure their endpoints are secure and only authorized users can gain access to their networks.

However, native support alone does not make for a secure operating system. Microsoft employs secure containers to ensure secure tokens are not attacked on the device, otherwise rendering multi-factor authentication worthless. By implementing secure containers, companies make it harder for hackers to steal the tokens used for authenticating the user on the device.

Microsoft enables multi-factor authentication through Windows Hello. This technology is designed to make logging into Windows 10 easier, but it is also used for secure multi-factor authentication. The system reads a person's face / finger, determines if it is an authorized identity, and then grants or denies access. Currently, only the Surface Pro 4, SurfaceBook, Windows 10 PCs with compliant fingerprint readers, and Intel RealSense cameras have Windows Hello capability.

NOT ALL MULTI-FACTOR AUTHENTICATION IS THE SAME

True multi-factor authentication is not just the combination of two single-factor authentication schemes. Having a password followed by an SMS message simply is not

secure enough. There are many ways such a system could be compromised; a user's device may be stolen, and thieves may log in once they have the device in their possession. SMS messages can be remotely intercepted and used to gain access, which compromises the security of the multi-factor authentication.

True MFA turns the PC into part of the answer to endpoint security issues instead of the cause. For example, combining a user's face with their fingerprint scan would be vastly harder to spoof or fool the system into granting access. With the latest 3D cameras and fingerprint scanners, fooling one of these devices is extremely difficult, but fooling both at the same time may actually be nearly impossible. Solutions like Intel Authenticate allow for different levels of security using different factors of authentication, based upon the network policies implemented by the administrator. Device security protocols can also be set depending on the type of network to which a user connects. Hackers will have to look for other vulnerable spots in a company's network if they come upon such a deployments of MFA.

Solutions Like Intel Authenticate Are More Reliable & Secure

Without a secure OS with the proper updates, no amount of hardware-level security is enough. The inverse is also true. No amount of software security is good enough without some form of hardware-level security to verify that the person at the PC is an authorized user. Secure hardware and secure software complement each other to deliver the best possible security and peace of mind.

By combining hardened in-hardware security with a software security platform, Intel Authenticate offers a superior solution on operating systems like Windows 10, Windows 8, or even Windows 7. Intel Authenticate sits below the OS, making remote software-level attacks much more difficult to execute, and it adds a physical layer of complexity to the security regime. Intel Authenticate helps make the endpoint part of the security solution rather than part of the problem.

Intel Authenticate embeds public key encryption at the hardware-level and makes tampering harder for an attacker. MFA solutions like Intel Authenticate rely on PKI (public key infrastructure), a system of hardware, software, policies and procedures that help to secure a network against external threats. Public key encryption in hardware ensures that there is a secure end-to-end method of transmitting encrypted data and can guarantee a certain level of security at the endpoint, be it a kiosk or a user's PC.

Intel Authenticate is in preview with select hardware and software partners but can be seen in some Lenovo systems using Synaptics' latest fingerprint sensor technology.

PCs with Single-Factor Authentication are a Vulnerability

Single-factor authentication regimes, like using a password only, are inherently insecure and dangerous. Enterprise IT managers who allow their users to authenticate using only passwords not only risk the security of their businesses but also risk their own job and possibly their career. The likelihood is high that hacked companies had poor authentication procedures that used single-factor authentication.[9]

Single-factor authentication, the old way, was never safe and never will be secure. Multi-factor authentication is the way to prevent stolen credentials from being used by an external attacker to further compromise the enterprise. Hardware-based MFA like Intel Authenticate further protects enterprises with an added level of protection from remote threats and offers the highest level of security in such scenarios.

Call to Action

Companies both big and small are breached on a daily basis, and millions of users' passwords and usernames are on the web.[10] Companies that do not use hardware-based, hardened multi-factor authentication like Intel Authenticate in conjunction with other layers of security run the risk increased exposure to an attack.

A data breach is no longer just an embarrassment for companies. There is a very high monetary cost associated with weak security procedures. Companies' executives are now fired for their poor security procedures and responses to data breaches.

Moor Insights & Strategy recommends that enterprise IT managers rapidly evaluate and use some form of hardened MFA technologies like Intel Authenticate to better secure their company from identity attacks.

REFERENCES

[1] http://www.sony.net/SonyInfo/News/Press/201105/11-0503E/index.html
[2] http://www.t-mobile.com/landing/experian-data-breach-faq.html
[3] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[4] http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/
[5] http://www.sony.net/SonyInfo/News/Press/201105/11-0503E/index.html
[6] http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151202
[7] https://corporate.target.com/press/releases/2014/05/statement-from-targets-board-of-directors
[8] http://content.randstadsourceright.com/talent-trends-report-2015
[9] http://www.cnbc.com/2015/11/04/cybersecurity-heres-why-companies-are-still-getting-hacked-commentary.html
[10] https://haveibeenpwned.com/

IMPORTANT INFORMATION ABOUT THIS PAPER

AUTHORS
Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy
Anshel Sag, Technical Writer at Moor Insights & Strategy

EDITOR
Scott McCutcheon, Director of Research at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

DISCLOSURES
This paper was commissioned by Intel. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.