TECH BRIEF

# CORE PRINCIPLES OF CYBER HYGIENE IN A WORLD OF CLOUD AND MOBILITY

## Achieving More Effective Security

Cybersecurity is a top concern at the highest levels of government and industry worldwide. More than ever, government and corporate leaders – from Senators and Members of Parliament to CEOs and Board Directors – are deeply engaged in ensuring effective cybersecurity strategies are in place at government agencies and companies. Yet as investments in cybersecurity accelerate, breaches continue to occur at an alarming frequency. Something is not working. What is it? And how do we fix it?

At VMware, we believe that more effective information security will be achieved by architecting security in rather than bolting it on as an afterthought. This has been inherently difficult to achieve, but new capabilities provided by cloud and mobile computing now make it feasible if not essential. Organizations can move to a more effective approach by taking two steps: implement basic cyber hygiene and focus on protecting the crown jewels – the mission critical business applications and data.

## Implement Basic Cyber Hygiene

We propose a set of core principles of cyber hygiene as a universal baseline: the most important and *basic* things an organization should have in place for cyber defense. The principles are not new concepts. They are rooted in well-established frameworks such as the NIST Cybersecurity Framework (CSF) and are technology-neutral. In the most devastating data breaches over the last few years – from Target to Sony to the U.S. Office of Personnel Management (OPM) – we firmly believe effectively adhering to these principles would have made a meaningful difference.

**MICRO-SEGMENTATION:**
Protecting the IT environment by breaking it up into smaller parts is similar to the use of compartments on a ship. It makes the ship easier to protect. If the ship is damaged in one area, the damage is contained to that area.

**THE CORE PRINCIPLES**

| | |
|---|---|
| The Underpinning: Education | Education must be firmly set as the cornerstone. A mandatory education process should be in place for IT professionals and end users. Like washing your hands and brushing your teeth, everyone should be educated and practicing the basics regularly. |
| 1. Least Privilege | Users should be allowed only the minimum necessary access needed to perform their job and nothing more. And system components should be allowed only the minimum necessary function needed to perform their purpose and nothing more. |
| 2. Micro-segmentation | The whole IT environment should be divided into small parts to make it more manageable to protect and to contain the damage if one part gets compromised (see diagram below). |
| 3. Encryption | For critical business processes, all data should be encrypted while being stored or transmitted. In the event of a data breach, stealing critical files should only result in obtaining unreadable data. |
| 4. Multi-factor Authentication | The identity of users and system components should be verified using multiple factors (not just simple passwords) and be commensurate with the risk of the requested access or function. |
| 5. Patching | Systems should be kept up to date and consistently maintained. Any critical system that is out of date is a meaningful security risk. |

## Focus On Protecting *Individual* Critical Applications

The next step is to focus on protecting an organization's "crown jewels." Examples include: an enterprise financial application that processes sensitive data in creating the company's financial statements; or an ordering application that fulfills customer orders, including storing personal information and credit card data. Until now, it has been difficult to focus on protecting individual applications. Modern applications are designed as distributed and dynamic systems. With current approaches, security tools are unable to identify that a particular group of software and hardware components is an individual application, and therefore unable to effectively protect it.

## Application-Focused Capabilities

Recent advances in cloud and mobile computing enable organizations to:

- Recognize an individual application and establish a baseline reference for it
- Compartmentalize system components into individual applications
- Position defenses around each individual application

## Effectively Implement the Core Principles

With an application-focused approach in place, it will be much easier to implement the core principles effectively.

| Principle | Application-focused approach | More effective implementation. |
|---|---|---|
| The Underpinning: Education | A mandatory education process should be in place for IT professionals and end users, with a focus on applications. | Education will be more relevant, tailored to the applications that IT professionals and/or users work with. |
| 1. Least Privilege | Users should be allowed only the minimum necessary access needed per individual application to perform their job and nothing more. System components should be allowed only the minimum necessary function needed per individual application to perform their purpose and nothing more. | User access and system component function will be more tightly controlled. It will be more difficult for attackers to find ways to gain access, alter processes, or hijack interactions (both "system to system" and "user to system"). |
| 2. Micro-segmentation | The whole IT environment should be divided into small parts by setting up boundaries around individual applications to make it more manageable to protect and to contain the damage if one part gets compromised. | Movement within the IT environment will be significantly inhibited. If attackers do make it into one part, they will be confined to a very small part (i.e. a single application), and find it difficult to reach other parts. |
| 3. Encryption | For critical business processes, all data should be encrypted while stored or transmitted by the components of an individual application. In the event of a data breach, stealing critical files should only result in obtaining unreadable data. | The distribution of the keys required to lock/unlock the data will be simplified since it is managed for each application individually. It will be more feasible to implement encryption comprehensively. |
| 4. Multi-factor Authentication | The identity of users and system components should be verified using multiple factors (not just simple passwords) and be commensurate with the risk of the requested access or function for an individual application. | Enforcing a risk-appropriate level of multi-factor authentication (MFA) for every request will be more feasible since it is managed per application. Attackers will find it more difficult to perform attacks if they can no longer simply steal or guess passwords. |
| 5. Patching | Systems should be kept up to date and consistently maintained based on the knowledge of each individual application. Any critical system that is out of date is a meaningful security risk. | Patching will be much easier to do consistently, knowing which application's components are affected and the possible impact to systems. Attackers will find it much harder to find vulnerable systems to exploit. |

This paper provides a brief summary of a more extensive white paper. Click here to download the full document.

vmware®

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com