BRIEF

Morphisec Exceeds MAS Criteria to Strengthen Cyber Resilience

Introduction

The scenario is a familiar one. We are attacked and react, adopting new regulations, adding more detection and reporting layers. In the process; we make it harder and costlier to run a secure business and make it harder to advance our business agenda. And we still get hit by the next, new threat. It's time to rethink this paradigm.

Morphisec is leading the charge to transform the way organizations approach cybersecurity. We suggest a new definition of "defense in depth" with a "fit for purpose" approach that radically decreases the risk exposure of enterprises while actually reducing costs, complexity, disruptions, and the "surprises" stemming from advanced cyber-attacks. As important, it enables critical OT and IT business processes to go on undisrupted, supporting the acceleration of digitization, virtualization, and business.

Background

In July 2018, Singapore suffered a massive data breach, whereby 1.5M private data records were compromised, including the Prime Minister's medical prescriptions. In the face of increasing cyberattacks, and with more financial processes being transacted digitally, the Monetary Authority of Singapore (MAS) issued a proposal on September 6 that strengthens the standard definition of "good cyber hygiene, defining six measures by which institutions will be bound legally and financially:

- *Addressing system security flaws in a timely manner*
- *Establishing and implementing robust security for systems*
- *Deploying security devices to secure system connections;*
- *Installing anti-virus software to mitigate the risk of malware infection;*
- *Restricting the use of system administrator accounts that can modify system configurations;*
- *Strengthening user authentication for system administrator accounts on critical systems.*

According to MAS, this move is aimed at countering cyber breaches, which are often the result of insecure system configurations or compromised system accounts. The proposed measures aim to enhance the security of financial institutions' systems and networks as well as mitigate the risk of unauthorized use of system accounts with extensive access privileges.

Unfortunately, regulations provide little defense against a clever attacker using unknown or highly advanced techniques. At the minimum level of compliance, none of the above measures would have prevented the infamous CCleaner attack which affected millions of Avast customers worldwide, including a critical port management corporation in Singapore. Only Morphisec, with its innovative Moving Target Defense approach to security, was able to stop the potentially devastating attack.

The Limits of Detection

The requirements laid out by MAS are important and essential. (In fact, we would even add a couple of items.) However, while we contend that these measures are critical, they do not help change anything in a transformational or material way.

Since the dawn of time, mankind has preferred the same method of defense. We put sentinels on the walls looking out for enemies. Before long, our enemies realize how to deceive with Trojans – so we put another defense line to watch for what is coming out of the Trojans. Once the enemies realize we can find that, they change what it looks like or how it behaves, so we put more and more detection lines. With each successive failure, we revert to blaming employees for being human, opening emails or attachments and normal human activities. This type of "defense in depth" is nothing more than lines of single points of eventual failure with the human as the last line of defense.

The inherent problems in this approach include:

1. Every defense line is a single point of failure, it either possesses the singular capability needed to detect an attack – be it signatures, knowledge, heuristics, etc. – or it doesn't and fails.

2. To compensate, vendors add service on top of service, each a single point of failure, and package them as a single agent. But this creates significant issues of complexity and performance degradation, patching and updates.

3. These defense lines can be easily defeated. Every defense line uses yesterday's knowledge to try to combat tomorrow's battle. Until they catch up, they are vulnerable.

4. This brand of defense-in-depth is no longer sustainable due to IT costs, disruptions, updates, false alarms, and continuous pursuit of ever changing attack forms. It is no longer scalable and there are not enough security experts to handle this. This is true for the large banks with enormous security spend, and even more true for the 80% of companies that simply do not have these kind of funds or personnel.

The Essence of Good Defense

This millennia-old security approach is missing the central tenet of Good Defense. A good defense puts in place strategies to prevent the attack from ever taking place. It makes sure that attackers never find what they are looking for. This is the basis of Moving Target Defense: it reduces the target surface to zero, so that rather than the defender chasing attackers, the attackers chase targets they can never find.

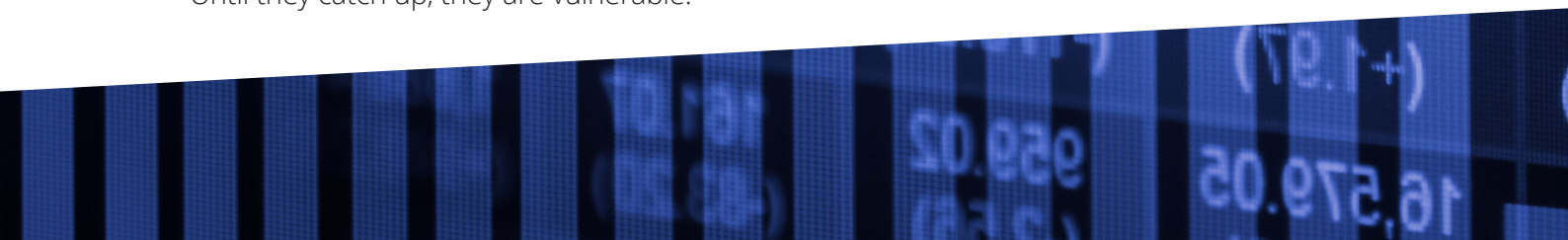
Four KPIs of an Optimal Security Stack

Time - Reduce any latency/dwell time to zero, stop attacks "before they are born."

Vectors – Focus on defending the pathways, rather than hunt, detect, and try to respond to billions of malware variants.

Simplicity – Build something that is manageable, requiring minimum IT and security resources. The most effortless stack possible – one focused on knowledge-free, update-free, attack preemption.

ROI – build the leanest stack (risk reduction per dollar spent) that gives you simultaneously the lowest residual risk and lowest Total Cost of Ownership (TCO).



How do the New MAS Measures Measure Up?

Looking at the six required measures, it is hard to identify anything that would bring about a real transformation in security practices. Let's review each of them vis-a-vis how cyber defense works today:

Addressing system security flaws in a timely manner

Certainly regular, timely patching is important. In an ideal world, organizations would patch security flaws as soon as a patch is released. But this is not feasible when patching is costly, disruptive to operations and even, as we saw with the Meltdown/Spectre patches, risky. And what about the unknown security flaws just waiting for a zero-day attack?

Establishing and implementing robust security for systems

This has the potential to be a significant force for change, depending on the definition of robust. What can companies do to establish truly robust and resilient security?

Deploying security devices to secure system connections

Every company should implement a good perimeter defense including gateways, "data diodes" and Network Access Control. It is a must for a cyber defense stack. But this does not address the unknown unknowns.

Installing anti-virus software to mitigate the risk of malware infection

Installing a good antivirus is a must for any business in order to handle the billions of known signatures and malware. However, antivirus is not effective against new variants and unknown attacks.

Restricting the use of system administrator accounts that can modify system configurations

Organizations should always be careful with the number of system administrators. However, this is of little help when privileges are stolen, escalated and can bypass these restrictions.

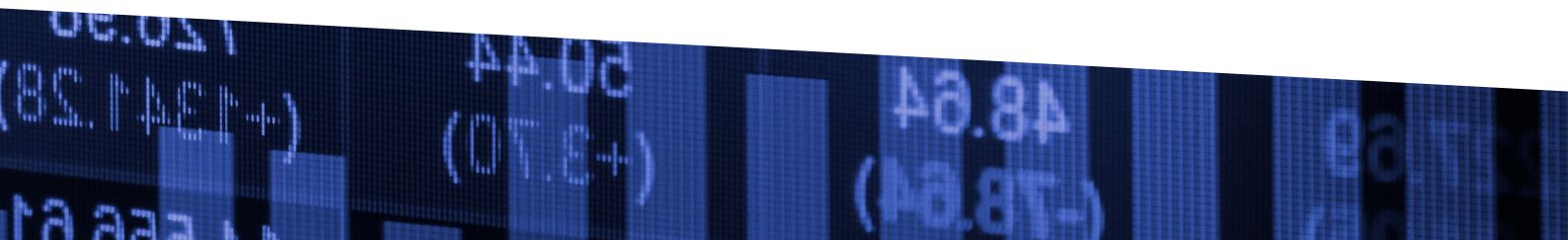
Strengthening user authentication for system administrator accounts on critical systems

Every company should implement a strong Access Management and Authentication policy and process – it is a must for a cyber defense stack. However, what should companies do in light of the following facts?

- The whole nature of advanced attacks is to escalate privileges without anyone knowing.
- The walls between critical and non-critical systems are crumbling with the progress of digitization, hence the attackers infiltrate through the weaker links and move laterally to more critical systems.
- Implementing extremely granular policies and controls is difficult and time-consuming.

The Verdict

Undoubtedly Network and Perimeter Defense, Access Management and Authorization and a good antivirus are necessary components of a robust stack. Companies that have not yet put in place these lines of defense should fix this. But we contend that the measures do little to really change the security posture of financial institutions and other regulated companies. And they do nothing to make them more successful in stopping modern highly evasive attacks and unknown, not-yet-seen threats.



Morphisec and MAS Measures: The Right Proposition

Morphisec leverages Moving Target Defense to provide the critical memory protection layer against advanced, polymorphic threats, which pose the most risk and cause the most damage. Morphisec can help Singapore companies reach and exceed the MAS requirements in a practical and cost effective manner.

- Morphisec stops attacks "before they are born or conceived." It forces attackers to look for targets they can never find, getting trapped at each step of their multiple attempts, cutting detection and response latency **Time** to **Zero**.
- Morphisec's Moving Target Defense technology destroys the attack pathways along their **Vectors** without the need for hunting, detecting or any prior knowledge. It keeps organizations protected during patching gaps by preventing exploitation of unpatched security vulnerabilities.
- It decreases the threat stemming from unknown unknowns, privilege escalation, AV bypass, Behavior bypass, AI bypass and Whitelisting bypass, with a single 2 MB service that requires no management and has zero performance penalty. It requires no prior knowledge and generates zero false alarms – true "set & forget" for maximum **Simplicity**.
- It forms the foundation that enables companies to build a simple stack with the **Lowest Total Cost of Ownership** and **Lowest Residual Risk**. Such a stack consists of:
  - ***Network Protection***
  - ***Access Management and Authorization Protection***
  - ***Morphisec for Memory Protection***
  - ***Known Virus Protection***

Protect Your Financial Institution From Advanced Threats

Morphisec is offered to Singapore customers through SECOM's ***EMS: Powered by Morphisec*** service. For more information contact salessup@secom.com.sg.

MORPHISEC
Moving Target Defense

www.morphisec.com

SECOM
SECURITY COMMUNICATION