Baseline Cloud Security - By Default

Freddy Dezeure

Who Am I?

- CIO in a private enterprise 1982-1987
- European Commission official 1987-2017
  - Founder and Head of CERT-EU 2011-2017
- Independent Advisor in cyber security and risk management
- Advisor in high-tech companies
- Community contributor



Main Cloud Service Providers

Managing the world's infrastructure

Cloud (IAAS): 70% market share

Office automation (SAAS): 100% market share

https://www.gartner.com/en/newsroom/press-releases/2024-07-22-gartner-says-worldwide-iaas-public-cloud-services-revenue-grew-16-point-2-percent-in-2023

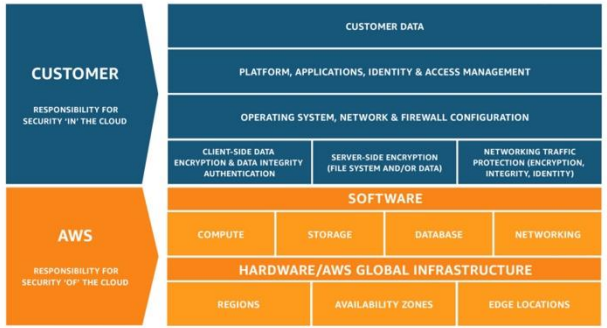
What's at Stake?

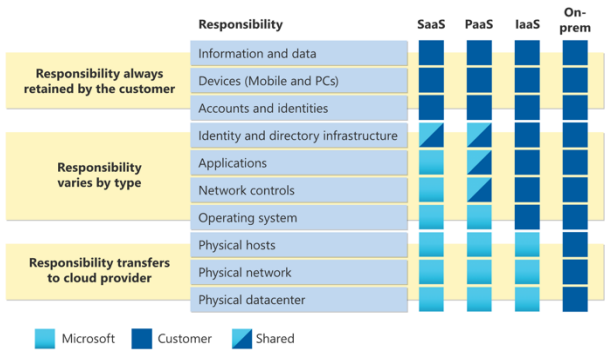
- Dependency on cloud infrastructure
  - Impact beyond a single organisation
  - High economic and societal reliance
  - National security / sovereignty

- Cloud architecture
  - Distributed, interconnected, accessible
  - Increasingly complex
  - Could be protected at scale

However…

- CSPs rely on customers to implement secure configurations, controls, and policies.
- Customers lack the expertise to do this.
- Most organizations are not / will never be secure.
- Thriving economy of criminals hacking our infrastructure and vendors promising to protect it.





Vendor guidance

https://learn.microsoft.com/en-us/microsoft-365/security/
https://www.microsoft.com/en-us/security
https://aws.amazon.com/security/
https://cloud.google.com/security
https://workspace.google.com/security/

Government guidance

SCuBA

FedRAMP

CyberFundamentals

Community guidance

CCM Cloud Controls Matrix

CIS Controls

CLOUD PROFILE

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
FS-ISAC
Principles for Financial Institutions' Security and Resilience in Cloud Service Environments

Users

Individual efforts to harden infrastructure:

- Internal expertise
- Paid vendor support
- Specialised consultancy

Vendors
Profit driven
Organised by product
Dealing with legacy
Concerned about legal risks – liability
Very resourceful, dominant

Governments – Regulators
Organised by sector
Slow and static
Lacking skills
Influenced by lobbyists
Scattered

Community
Loosely organised
Mostly representing mature organisations
Lack of corporate (legal) weight
Scattered

Users
Cost driven
Focused on convenience and business value
Lacking skills, uninformed, underresourced
Dealing with legacy
Scattered

EU Cyber Resilience Act

Products with a digital component should "be delivered with a secure default configuration, including the possibility to reset the product to its original state "

This Regulation ensures a high level of cybersecurity of products with digital elements. It does not regulate services, such as Software-as-a-Service (SaaS)…

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454

US National Cybersecurity Strategy

"We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us."

https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Federal Office for Information Security

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre

National Cyber Security Centre
Ministry of Justice and Security

National Cyber Security Centre

CSIRTAmericas Network

NISC

CSA SINGAPORE

certnz

NSM
NORWEGIAN NATIONAL CYBER SECURITY CENTRE

National Cyber and Information Security Agency

KISA KOREA INTERNET & SECURITY AGENCY

JPCERT CC®

Within a year, demonstrate measurable progress in the following areas:

1. **Increase the use of multi-factor authentication (MFA).**
2. **Reduce default passwords across products.**
3. **Reduce entire classes of vulnerabilities.**
4. **Increase the installation of security patches by customers.**
5. **Publish a vulnerability disclosure policy (VDP).**
6. **Transparency in vulnerability reporting.**
7. **Increase in the ability for customers to gather evidence of intrusions.**

More

"We strongly encourage manufacturers to improve the security of products throughtout their life cycle and make them secure-by-design and secure-by-default"

https://www.consilium.europa.eu/media/fttjqncg/apulia-g7-leaders-communique.pdf

Security by Default/Design: "One Click" Security for cloud workloads

https://www.fsisac.com/hubfs/Knowledge/Cloud/PrinciplesForFinancialInstitutionsSecurityAndResilienceInCloudServiceEnvironments.pdf

Our Call to Action

Improving the world's cyber resilience, at scale

Implementing baseline security by default

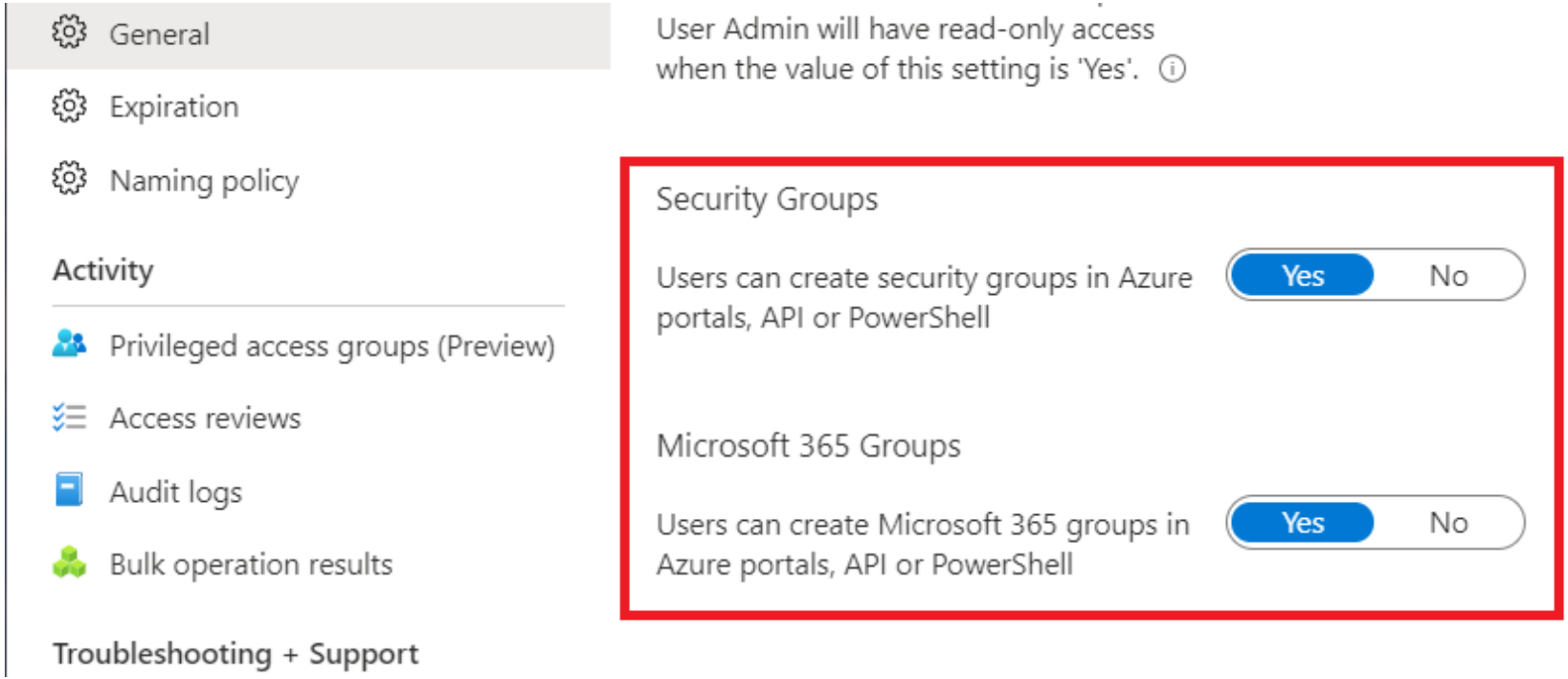
Freddy Dezeure, Prof. Lokke Moerel, and Dr. George Webster

Calling upon CSPs to **apply** baseline enterprise cybersecurity and resilience principles **in the user infrastructure** by **default**.

Moving from "opt-in" to "built-in/opt-out".

https://www.researchgate.net/publication/378213351_Improving_the_world's_cyber_resilience_at_scale_Implementing_baseline_security_by_default

Recent Red Team



CIS Microsoft Azure Foundations v2.1.0 L2

Download File

Audit Details

Name: CIS Microsoft Azure Foundations v2.1.0 L2

Updated: 7/22/2024

Authority: CIS

Plugin: microsoft_azure

Revision: 1.2

Estimated Item Count: 56

File Details

Filename:
CIS_Microsoft_Azure_Foundations_v2.1.0_L2.audit

Size: 253 kB

MD5: 5643765866e1cbd7026c7b3aa8b48a7c

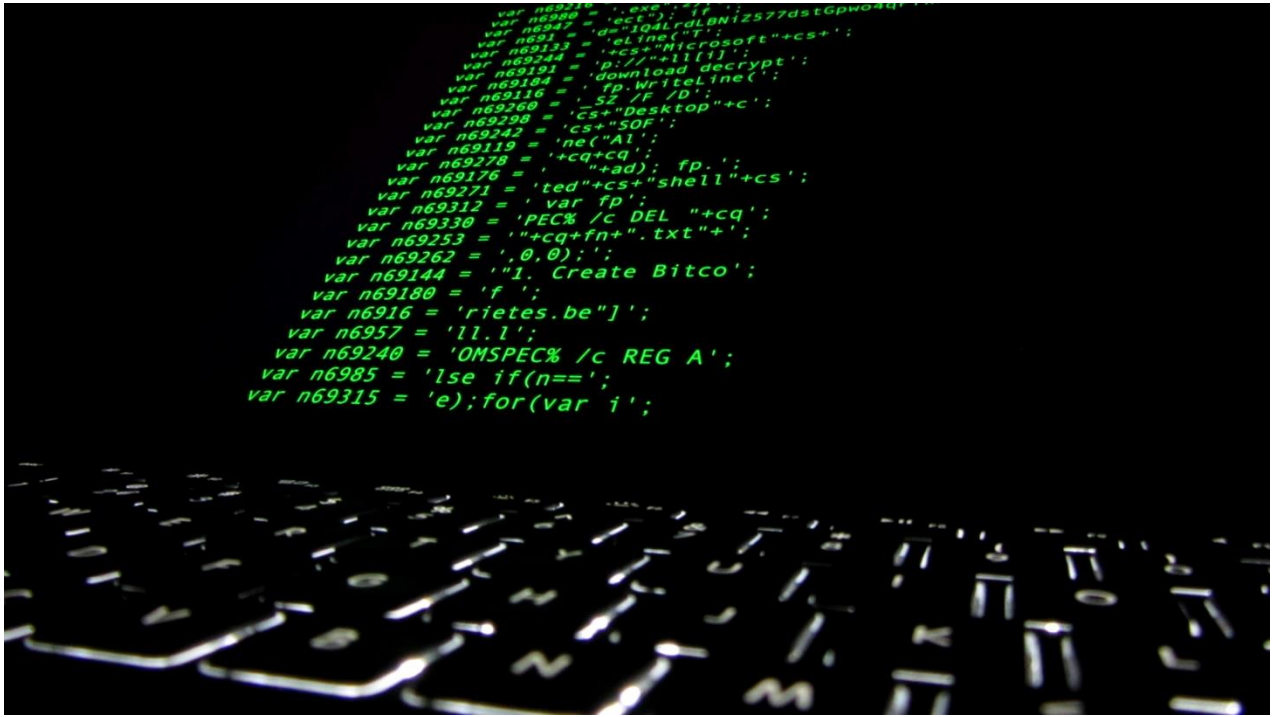
SHA256:
8005eb0ad64c7dd33081709b32303dddd1c5760f27a78f067b3f804c0003a229

Audit Items

Items | Changelog

Description	Categories
1.1.3 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users	IDENTIFICATION AND AUTHENTICATION
1.11 Ensure 'User consent for applications' Is Set To 'Allow for Verified Publishers'	ACCESS CONTROL, CONFIGURATION MANAGEMENT, IDENTIFICATION AND AUTHENTICATION
1.15 Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	ACCESS CONTROL, AUDIT AND ACCOUNTABILITY, IDENTIFICATION AND AUTHENTICATION
1.17 Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes'	ACCESS CONTROL, AUDIT AND ACCOUNTABILITY
1.18 Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	ACCESS CONTROL, AUDIT AND ACCOUNTABILITY

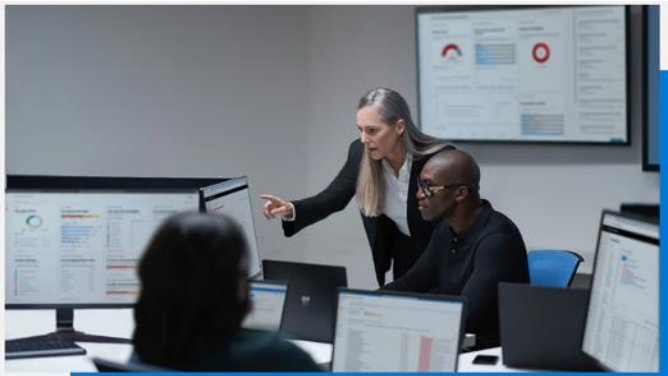
How about your Backup?



Main Points of our Call

- Addressing the complexity of cloud infrastructure;
- Focusing on user infrastructure rather than on individual products;
- Adapting to threat landscape;
- Vendors set the default, using industry best practices;
- Built-in/opt-out instead of opt-in.

Threat-Informed



Research Threat intelligence Microsoft Defender

Threat actors

10 min read

Midnight Blizzard: Guidance for responders on nation-state attack

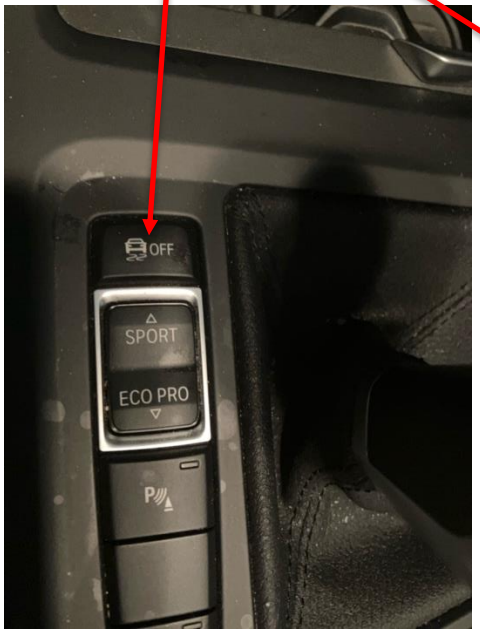
By Microsoft Threat Intelligence

January 25, 2024

more

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM. The latest information from the Microsoft Security and Response Center (MSRC) is posted here.

Built-in / opt-out



Tiered Approach

1. Secure baselines implemented by default, at no additional cost.
2. If (1) is not possible, secure baselines implemented *by workflow*.
3. Transparently explained opt-in services (*e.g.*, logging and secure backups).

User organizations can still raise their protection to a higher level if they wish. Those opting out of secure baselines may expose themselves to a higher risk and additional scrutiny from regulators and insurers.

Proposed Next Steps

- Strengthen community support (you)
- CSP Working Group to define default cloud baselines
- Community Stakeholder Group to challenge/validate
- Facilitated by CISA and ENISA

Thank You

https://www.FreddyDezeure.eu/