Михаил Кадер
архитектор по информационной безопасности

Удаленный доступ – доколе?

Удаленный доступ все еще неизбежная реальность?

Пандемия?

Цифровые бедуины?

Экономия?

Что еще?

Amazon

Безос перевел Амазон на 5-дневную офисную рабочую неделю (https://www.cnbc.com/2024/09/16/amazon-jassy-tells-employees-to-return-to-office-five-days-a-week.html)

- С января 2025 все работают 5 дней из офиса, а не 3, как было в этом году
- Исключения могут согласовать лично только топ-30 руководителей компании
- Амазон хочет работать как стартап
- Бюрократия будет выжигаться, в том числе через специальный канал связи, куда о ней можно сообщить
- Часть менеджеров уволят, чтобы на 15% увеличить долю инвестиционного капитала
- Всю структуру будут уплощать

Шутки шутками ...

Jameson Zaballos • 3rd+

Co-founder at Napa | Memes for ...

1w •

+ Follow

Everyone calm down. Amazon is still a hybrid company.

Monday-Friday: In-office
Saturday and Sunday: Work from home

27,582

288 comments • 155 reposts

Удаленный доступа как элемент атаки на цепочки поставок

Связанные атаки на Marquard & Bahls, SEA-invest, Evos едва не оставили Европу без нефтепродуктов

Успешная атака на одно предприятие холдинга иногда способно остановить все производство холдинга

Киберустойчивость предприятия

Набор функций (сервисов) ИБ, распределенных между внутренними и внешними **командами** (сотрудниками), который **описан через десятки процессов** стратегического, тактического и оперативного уровня и **реализован с использованием технологий** детектирования, анализа, корреляции и реагирования для обеспечения невозможности наступления **недопустимых событий**

Недопустимое событие

Недопустимое событие — событие, делающее невозможным достижение операционных и (или) стратегических целей или приводящее к значительному нарушению основной деятельности организации в результате кибератаки.

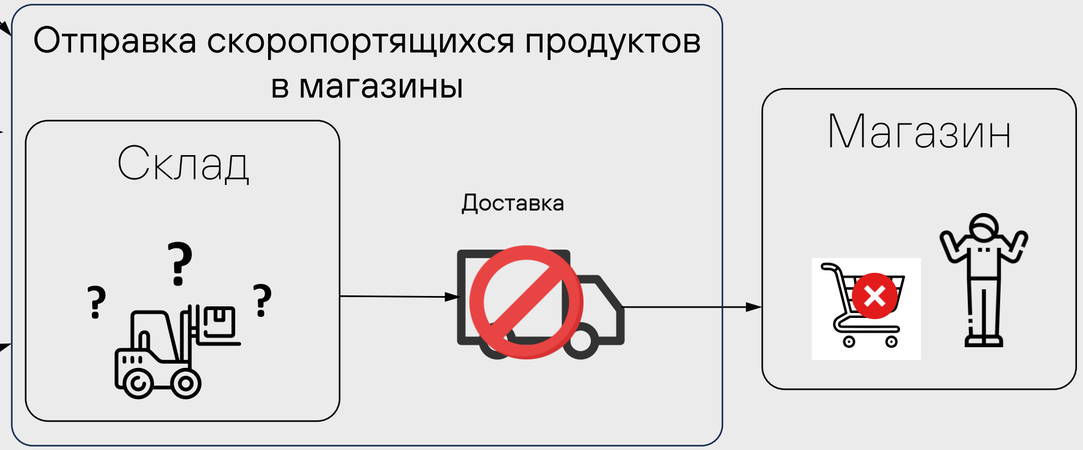
Такое событие может произойти по разным сценариям:

Сценарий 1: Нарушение комплектования заказов

Сценарий 2: Нарушение перевозок

Сценарий 3: прерывание управления складом

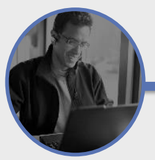
Пример недопустимого события: нарушение доставки скоропортящихся продуктов на срок более 48 часов.



Сценарий #3 нацелен на прерывание работы системы управления складом путем удаления или шифрования данных в системе и резервных копий.

Удаление всех данных (включая бэкапы) системы управления складом гарантирует прерывание приёма товаров на склад и их отправки на срок, превышающий 60 часов.

Риски удаленного подключения



Удаленное рабочее место

Взаимодействие – Устройства/Пользователи к приложениям и Администраторы для управления ими

Риски – Недостаточная осведомленность, незащищенные соединения, нарушения политик, уязвимости, ВПО, взлом

Приложения

Тепловая карта MITRE ATT&CK

Визуализация наиболее популярных техник и подтехник, которые используют эксперты Positive Technologies.

Initial Access		Execution		Persistance		Privilege Escalation		Defense Evasion		Credential Access		Discovery		Lateral Movement		Collection		Command and Control	
Exploit Public-Facing Application		Command and Scripting Interpreter	JavaScript	Account Manipulation	SSH Authorized Keys	Abuse Elevation Control Mechanism	Sudo and Sudo Caching	Access Token Manipulation	Create Process with Token	Adversary-in-the-Middle	ARP Cache Poisoning	Account Discovery	Domain Account	Exploitation of Remote Services		Adversary-in-the-Middle	ARP Cache Poisoning	Application Layer Protocol	Web Protocols
External Remote Services			PowerShell	Create Account	Domain Account	Access Token Manipulation	Create Process with Token		SID-History Injection		LLMNR/NBT-NS Poisoning and SMB Relay		Email Account	Lateral Tool Transfer			LLMNR/NBT-NS Poisoning and SMB Relay	Data Encoding	Non-Standard Encoding
Phishing			Python		Local Account		SID-History Injection		Token Impersonation/Theft	Brute Force	Credential Stuffing		Local Account	Remote Service Session Hijacking	SSH Hijacking	Archive Collected Data	Archive via Utility		Standard Encoding
Supply Chain Compromise	Compromise Software Dependencies and Development Tools		Unix Shell	External Remote Services			Token Impersonation/Theft	Deobfuscate/Decode Files or Information			Password Cracking	Cloud Infrastructure Discovery		Remote Services	Distributed Component Object Model	Data from Configuration Repository	Network Device Configuration Dump	Encrypted Channel	Asymmetric Cryptography
Valid Accounts	Default Accounts		Windows Command Shell	Scheduled Task/Job	At	Domain Policy Modification	Group Policy Modification	Domain Policy Modification	Group Policy Modification		Password Guessing	Container and Resource Discovery				Remote Desktop Protocol		SNMP (MIB Dump)	Ingress Tool Transfer	
	Domain Accounts	Container Administration Command			Scheduled Task	Exploitation for Privilege Escalation		Exploitation for Defense Evasion			Password Spraying	Domain Trust Discovery			SMB/Windows Admin Shares	Data from Information Repositories	Code Repositories	Protocol Tunneling	
	Local Accounts	Exploitation for Client Execution		Server Software Component	Web Shell	Scheduled Task/Job	At	Impair Defenses	Disable or Modify System Firewall	Credentials from Password Stores	Password Managers	File and Directory Discovery			SSH		Confluence	Proxy	External Proxy
		Scheduled Task/Job	At	Valid Accounts	Default Accounts		Scheduled Task		Downgrade Attack	Exploitation for Credential Access		Group Policy Discovery			VNC		Sharepoint		Internal Proxy
		Software Deployment Tools	Scheduled Task		Domain Accounts	Valid Accounts	Default Accounts	Indicator Removal on Host	File Deletion	Forced Authentication		Network Service Discovery		Software Deployment Tools		Data from Local System		Remote Access Software	
					Local Accounts		Domain Accounts	Indirect Command Execution		Forge Web Credentials	Web Cookies	Network Share Discovery		Use Alternate Authentication Material	Pass the Hash				
							Local Accounts	Masquerading	Double File Extension	OS Credential Dumping	/etc/passwd and /etc/shadow	Network Sniffing			Pass the Ticket				
									Masquerade Task or Service		Cached Domain Credentials	Password Policy Discovery			Web Session Cookie				
								Modify Registry			DCSync	Permission Groups Discovery	Domain Groups						
								Use Alternate Authentication Material	Pass the Hash		LSA Secrets		Local Groups						
									Pass the Ticket		LSASS Memory	Process Discovery							
									Web Session Cookie		Security Account Manager	Query Registry							
								Valid Accounts	Default Accounts	Steal or Forge Kerberos Tickets	AS-REP Roasting	Remote System Discovery							
									Domain Accounts		Golden Ticket	Software Discovery							
									Local Accounts		Kerberoasting	System Information Discovery							
											Silver Ticket	System Network Configuration Discovery							
										Steal Web Session Cookie		System Network Connections Discovery							
										Unsecured Credentials	Bash History	System Owner/User Discovery							
											Cloud Instance Metadata API	System Service Discovery							
											Container API								
											Credentials In Files								
											Credentials in Registry								
											Private Keys								

Доля компаний в которых использовались техники и подтехники:

- 66%-100%
- 41%-65%
- 21%-40%
- 1%-20%

* https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2021-2022/

Пару слов напоследок

Тема
бесконечная

Предотвращение
недопустимых
событий как
основное
целеполагание

Никого «святого»

Пообсуждаем?