

Най-големите предизвикателства в киберсигурността за 2022 година

Димитър Радев

Ръководител отдел “Информационна сигурност и инфраструктура”

ТехноЛогика

dradev@technologica.com



Киберсигурност от ТехноЛогика

- **Експертиза**

- Изграждане и внедряване на широк спектър системи за сигурност
- Оценка на информационната сигурност
- Тестове за проникване – penetration testing
- Сертифициран екип

- **Партньори**

- Sophos
- Cisco, CheckPoint
- F5 Networks
- Thycotic / Delinea, CyberArk
- Microsoft
- EC-Council
- IBM, VMware и др.



Microsoft
Partner

Gold Application Integration
Gold Data Analytics
Gold Application Development
Gold Datacenter



Динамика в киберсигурността

- 27.05.2022 – Открит е документ, използващ не-документирана уязвимост (Zero Day) в Microsoft Word
 - Позволява незабелязано изпълнение на зловреден код
 - Използва Microsoft Troubleshooting wizards
 - Кръстена е Follina
- 31.05.2022 – Microsoft публикува workaround, но не и patch
- 05.06.2022 – Появяват се следните заглавия:



An Actively Exploited Microsoft Zero-Day Flaw Still Has No Patch

State-Backed Hackers Exploit Microsoft 'Follina' Bug to Target Entities in Europe and U.S

Zero-day уязвимости

- Уязвимост, известна на атакуващите преди разработчиците да са имали възможност да разработят patch или да знаят за нея
- Може да бъде използвана злонамерено и да не бъде открита дълго време – дни, месеци или години
- Атакуващите я експлоатират свободно докато тя не стане известна на разработчиците и обществеността
- Организациите трябва да внедрят мерки, за да се защитят от нея

Security awareness and training

- Потребителите са най-слабото звено в киберсигурността
 - Администраторите/привилегировани потребители са едно от най-критичните
- Стават причина за най-много успешни атаки
- Фишинг, социално инженерство
- Използване на еднакви пароли за лични и служебни нужди
- Дори да има редовни обучения, не винаги са ефективни
 - Еднообразни click-through обучения
 - Обучения с лектор, насочени към актуалните атаки и профилирани спрямо ролите на обучаемите
- Информираност на администраторите и служителите по киберсигурност – Twitter, форуми и групи за сигурност и др., CERT

Автентикация - Идентичност - Проследимост

- Все повече продукти и услуги се предоставят чрез облачен модел
- Как протича логин процеса в облачните услуги?
 - Office 365 използва много различни адреси
- Да се доверим ли на зеленото катинарче в браузъра?
 - Разлика между конфиденциалност и довереност
- Multi-Factor Authentication е задължителен елемент
- PAM - Privileged Account Management

Планове за реакция при инциденти

- Трябва да са разработени такива за различни сценарии
- Периодични тестове
- Бекъпите и архивите не са решение на всички проблеми
- Redundancy и High Availability на системите и процесите
 - Осигурява възможност важните бизнес процеси да могат да продължат да се изпълняват след атака



Обновяване и настройки по подразбиране

- Опитът ни показва, че обновяването не е достатъчно разпространено
- В практиката ни на оценка на сигурността откриваме системи с уязвимости, за които има обновления от години
- Новите уязвимости започват да се експлоатират, обикновено до 24 часа след като станат известни
- Настройките по подразбиране са публично известни и са един от първите вектори за атака



Атаки срещу ОТ (Operational Technology)

- ОТ - Изпълнението на физически процеси и машините нужни за това
- PLCs, SCADA, CCTV, CAM
- Много по-често сигурността при тях се negliжира отколкото при IT системите
- Атакуващите могат да внедрят зловреден код и системите да изпълняват желанията от тях действия или да предоставят грешни данни
- Тези атаки често могат да причинят физически щети



Атаки от веригата за доставки

- Managed Service Provider – Предоставят IT услуги на своите клиенти
 - Когато те станат жертва на атака, техните клиенти също са уязвими чрез каналите за управление.
- Доставчици и производители на софтуер – компрометирани обновления
- Доставчици на ресурси нужни за производството
- Зависимост от друга организация – увереност в бързината и на възстановяване след атака

Войната между Русия и Украйна

- Ransomware атаки
 - Conti – групировка, оперираща като бизнес. Има HR отдел, атестации и служител на месеца
 - Сама става жертва на желанието си да подкрепи една от страните и се налага да се ребрандира
- Атаки срещу критичната инфраструктура и веригата за доставки
- Възможно е да станете цел на APT (Advanced Persistent Threat)/State-sponsored attacker
 - Особено ако производството ви е свързано с военната промишленост



Продукти и системи за сигурност от ТехноЛогика

- Next Generation firewall + Intrusion Prevention System (IPS)
- Endpoint security – защита на крайните точки/работни станции
- Security Incident and Event Management – SIEM
- Privileged Account Management (PAM)
- Data Loss Prevention
- Email security
- Web Security Gateway
- Vulnerability management
- Patch management



Услуги - Оценка на киберсигурността

- Оценка на информационната инфраструктура от гледна точка на киберсигурността
- Оценка и подобряване на информационната сигурност на уеб сайтове/приложения и услуги, десктоп и мобилни приложения
- Прилагане на принципите за сигурност на приложенията
- Извършване на статичен и динамичен анализ на сигурността на приложенията и кода
- Pentesting – анализ на инфраструктурата и извършване на симулирани атаки с цел тестване на приложенията и инфраструктурата на клиента за възможности за пробиви

Услуги - Оценка на киберсигурността

- Реакция при кибер-инциденти и заплахи
- Оценка на състоянието, оценка и отстраняване на пробиви в сигурността на ИТ системи
- Премахване на зловреден код
- Възстановяване на работоспособността



Киберсигурността в 3DEXPERIENCE Cloud Platform

- Предимства на облачните услуги – скорост и ефективност
- Интелектуалната собственост на клиентите и данните на потребителите, включително личните данни, са защитени
- Система за сигурност, имплементирана на база на добрите практики
- ISO 9001:2015, ISO/IEC 27001:2017 и ISO/IEC 27701:2019 сертификация
- Secure Software Development Lifecycle методология
- Система изградена според препоръките на OWASP и NIST SP 800-53 стандарта
- <https://discover.3ds.com/cloud-security-data-privacy>



Благодаря за вниманието

Въпроси?