Acronis | softico

Тенденції кібербезпеки 2021

Рекомендації Acronis щодо забезпечення безпеки в умовах нинішніх і майбутніх загроз

Адаптовано компанією **SOFTICO**
www.softico.ua

Зростання кількості атак на віддалених працівників

Оскільки число випадків зараження COVID-19 швидко зростає, важко уявити, що пандемія закінчиться в цьому році. Більш ймовірно, що знадобиться увесь рік і, можливо, навіть 2022 рік, щоб вакцина поширидась по всьому світу. Це означає, що користувачі, що працюють віддалено, і досі залишаються погано захищеними. У 2020 році кіберзлочинці зрозуміли, що фішинг, як і раніше працює дуже добре і що співробітники - це доступ до даних компаній. Ми очікуємо, що кількість та якість атак на таких працівників буде рости, оскільки все більше кіберзлочинців прагнуть дістатися до бізнес-даних і систем.

Крадіжки даних переважатимуть над шифруванням даних

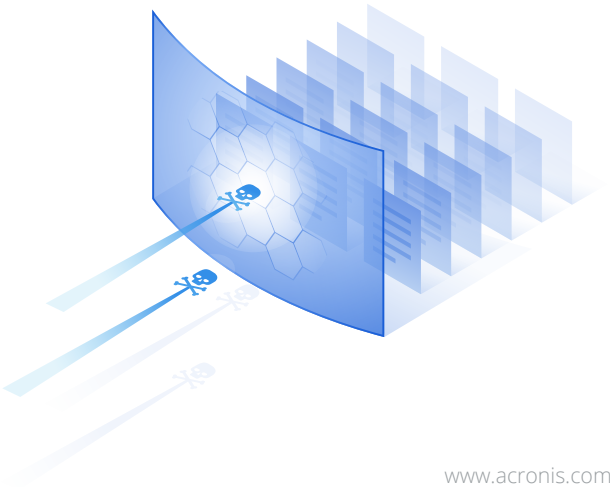
Нещодавні атаки ransomware показали, що кіберзлочинці мають на меті монетизувати кожну атаку.
Більш того, хакери переконались в тому, що вимагання з використанням вкрадених конфіденційних даних діє на жертв, можливо, навіть краще, ніж коли вони просто шифрують ті ж дані.
Тому ми очікуємо, що головною метою кожної атаки ransomware стане витік даних. Рішення по захисту даних і запобігання їх втрати будуть дуже важливі в наступному році, тому що навіть якщо ми побачимо зменшення кількості нових атак ransomware, вони будуть наносити величезної шкоди і будуть дуже успішними. Це означає, що в наступному році ми очікуємо, що ransomware як і раніше буде загрозою номер один для підприємств.

Більше нападів на MSP та малий бізнес

Оскільки все більше малих і середніх підприємств використовують хмарні MS(S)Ps, все більше кіберзлочинців можуть атакувати їх.
У 2019-2020 роках зловмисники зрозуміли, що атакувати MSP дуже вигідно, особливо невеликі компанії. Крім того, вони можуть використовувати добре відомі інструменти, такі як віддалений доступ і засоби доставки програмного забезпечення. Ці типи атак швидше за все, будуть рости в кількості і географії, оскільки як малі підприємства, так і MSP не готові до серйозних атак і все ще готові заплатити помірний викуп.

Атаки на хмари

Під час локдауну багато компаній перенесли свої сервіси в хмару. На жаль, конфігурація часто виконувалася поспішно і тому не була абсолютно безпечною, залишаючи хмарні додатки і служби даних відкритими для для всіх бажаючих в Інтернеті. Такий сценарій надає зловмисникам можливість отримати доступ до даних і поширити їх, як ми вже бачили у випадках витоку даних зі сховищ даних S3 і баз даних гнучкого пошуку. Крім того, управління ідентифікацією та доступом все ще часто ігнорується, хоча ідентифікаційні дані стають новим периметром. Така ситуація призводить до зростання моніторингу поведінки користувачів та впровадження систем динамічного контролю доступу.



Ransomware шукає нові цілі

Атаки Ransomware виходять за рамки настільних комп'ютерів Windows і Mac. Зловмисники намагаються закріпитися в хмарному середовищі, оскільки хмарні бази даних і контейнери є для них прибутковою метою. Всередині організацій все більш вразливі промислові системи управління (ICS) є ще однією цікавою ціллю. Для домашніх користувачів впровадження Інтернету речей (IoT), особливо зв'язку 5G, може створити нові області для зараження - навіть якщо просто для створити DDoS-атак як спосіб спонукати жертву заплатити викуп.

Атаки стають все більш автоматизованими, кількість видів шкідливого ПЗ зростає

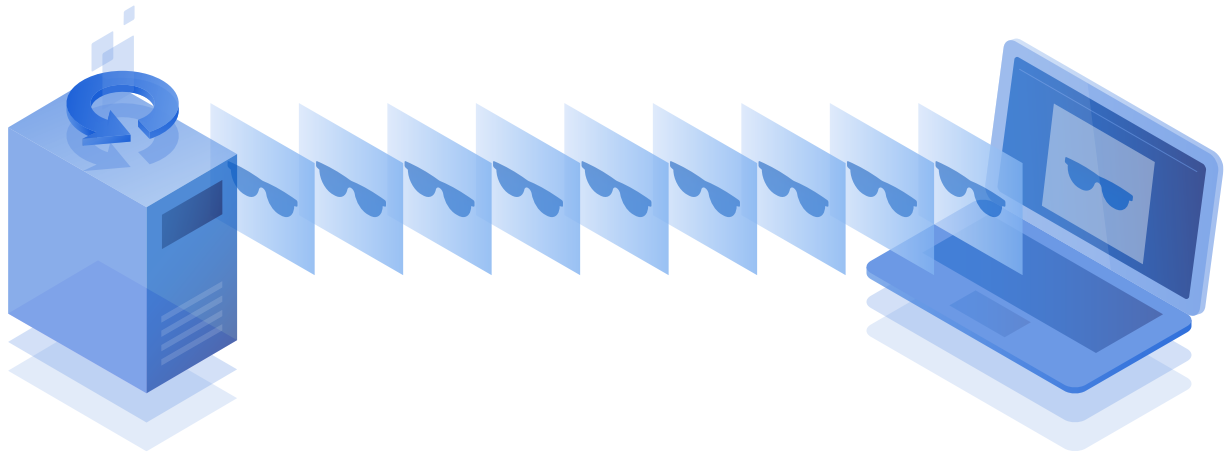
Кіберзлочинці намагаються автоматизувати свій процес всюди, де це можливо. Аналітика великих даних і машинне навчання дозволяють їм знаходити нових жертв і генерувати персоналізовані спам-повідомлення. Програми crimeware as a service і програми affiliate ще більше нарощують темпи поширення.
Однак після етапу первинного доступу і виконання, більшість атак як і раніше використовують ручні методи для поширення шкідливого ПЗ в мережах корпорацій. Тим не менш, ми будемо спостерігати більш часте використання вже відомих методів атак з різним рівнем персоналізації.

Рекомендації Acronis: як залишатися в безпеці в умовах існуючих і майбутніх загроз

Сучасні кібератаки, витік даних і спалах ransomware свідчать про те, що кібербезпека дає збої. Цей провал є результатом слабких технологій і людських помилок, викликаних розумною соціальною інженерією. У тих випадках, коли рішення для резервного копіювання працювало справно і не було скомпрометовано, на відновлення систем (з даними) до робочого стану зазвичай йдуть години та дні. Резервне копіювання необхідно в тих випадках, коли рішення з кібербезпеки дають збій, але в той же час рішення для створення резервної копії можуть бути скомпрометовані, відключені і працювати повільно, в результаті чого компанії втрачають багато грошей через простій.
Для вирішення цих проблем ми рекомендуємо інтегроване рішення кіберзахисту, таке як Acronis Cyber Protect, оцінка вразливостей, управління виправленнями, RMM і можливості резервного копіювання в єдиному агенті, що працює під управлінням операційних систем Windows. Така інтеграція дозволяє підтримувати оптимальну продуктивність, усувати проблеми сумісності та забезпечувати швидке відновлення.
Якщо загроза пропущена або виявлена під час зміни ваших даних, агент негайно відновить незмінені дані з резервної копії. Таке автоматичне відновлення неможливе за допомогою агента захисту від шкідливих програм. Ваше рішення для захисту від шкідливих програм може зупинити загрозу, але деякі дані можуть бути вже втрачені. Агент резервного копіювання не дізнається про це автоматично, і дані будуть відновлюватися повільно - якщо взагалі будуть відновлені.

Acronis Cyber Protect Cloud, в свою чергу, прагне зробити відновлення даних непотрібним, виявляючи і усуваючи загрози до того, як вони зможуть завдати шкоди вашому середовищу. Цей рівень захисту досягається завдяки нашій розширеній багаторівневій функціональності кібербезпеки.

Проте, компаніям і домашнім користувачам не варто забувати про основні правила безпеки, навіть якщо вони використовують такі сучасні рішення, як Acronis Cyber Protect.



Встановлюйте патчі для ОС і додатків

Установка патчів має вирішальне значення, оскільки багато атак здійснюються через невиправлені вразливості. Використовуючи Acronis Cyber Protect, ви отримуєте вбудовані функції оцінки вразливостей та управління виправленнями. Ми відстежуємо всі виявлені вразливості та випущені патчі, що дозволяє адміністраторам або технічним фахівцям легко встановлювати виправлення на всі кінцеві точки за допомогою гнучкої конфігурації та докладної звітності. Acronis Cyber Protect підтримує не тільки всі вбудовані додатки Windows, але і більш 100 популярних сторонніх додатків, включаючи такі інструменти, як Zoom і Slack та популярні VPN-клієнти, які використовуються при віддаленій роботі.

Якщо у вас немає Acronis Cyber Protect та / або ви не використовуєте програмне забезпечення для управління виправленнями, то це може спричинити нові проблеми. Як мінімум, необхідно переконатися, що Windows отримує всі необхідні оновлення та вони своєчасно встановлюються. Користувачі схильні ігнорувати системні повідомлення, особливо перезавантаження Windows, що є великою помилкою. Переконайтеся, що автоматичні оновлення популярних виробників програмного забезпечення, таких як Adobe, увімкнені, а такі додатки, як Acrobat Reader, також оновлюються оперативно.

Будьте готові до спроб фішингу

COVID-19 сьогодні широко використовується в спробах фішингу, але кількість таких атак і надалі буде тільки рости, тому кожен віддалений працівник повинен бути до них готовий. Тематичні фішингові і шкідливі веб-сайти з'являються у великій кількості щодня, вони зазвичай фільтруються на рівні браузера, але з такими рішеннями кіберзахисту, як Acronis Cyber Protect, ви також отримуєте спеціальну функцію фільтрації URL. Аналогічна функціональність доступна в рішеннях для захисту кінцевих точок, хоча в Acronis Cyber Protect є спеціальна категорія, пов'язана з темами громадської охорони здоров'я,

яка оновлюється з великим пріоритетом. Шкідливі посилання можуть надходити звідки завгодно, включаючи електронну пошту, повідомлення на форумах і додатки для обміну миттєвими повідомленнями. Не переходьте за посиланнями, які ви не очікували отримати.
Фішингові або шкідливі вкладення можуть надходити і через електронну пошту. Що стосується вкладень: завжди перевіряйте, звідки вони приходять, і запитуйте себе очікуєте ви його чи ні. У будь-якому випадку, перш ніж відкрити вкладення, його слід просканувати за допомогою вашого антивірусного рішення.

Використовуйте VPN при роботі з даними

Незалежно від того, підключаєтеся ви до віддалених джерел і сервісів компанії, або ваша робота не вимагає такої діяльності, і ви просто переглядаєте деякі веб-ресурси, завжди використовуйте віртуальну приватну мережу (VPN).
VPN шифрує весь ваш трафік, роблячи його безпечним на випадок, якщо хакер спробує перехопити ваші дані при передачі. Якщо у вашій компанії існує процедура VPN, то, швидше за все, ви отримаєте інструкції від адміністратора або технічного фахівця MSP. Якщо ви повинні забезпечити безпеку свого робочого місця самостійно, використовуйте добре відомі, рекомендовані програми та служби VPN, які широко доступні на ринку програмного забезпечення або безпосередньо у постачальників.

Переконайтеся, що ваше рішення з кібербезпеки працює правильно

У Acronis Cyber Protect ми використовуємо безліч збалансованих і тонко налаштованих технологій захисту, включаючи кілька систем виявлення - рекомендується замість вбудованого рішення для Windows.

Але просто встановити захист від шкідливого ПЗ недостатньо, його необхідно правильно налаштувати. Це означає, що:

- Повне сканування повинне виконуватися як мінімум кожен день.

- Продукт повинен отримувати оновлення щодня або щогодини, в залежності від того, як часто вони доступні.

- Продукт повинен бути підключений до своїх хмарних механізмів виявлення, в разі Acronis Cyber Protect - до Acronis Cloud Brain. За замовчуванням він включений, але вам необхідно переконатися, що інтернет доступний і випадково не заблокований антивірусним ПЗ.

- Сканування на вимогу і по доступу (в реальному часі) має бути включено і реагувати на кожне нове встановлене або програмне забезпечення, що виконується.

Крім того, не ігноруйте листи, що надходять від вашого рішення для захисту від шкідливих програм. Уважно читайте їх і переконайтеся, що ліцензія є законною, якщо ви використовуєте платну версію від постачальника засобів захисту.

Зберігайте свої паролі під надійним захистом

Остання порада з безпеки: переконайтеся, що ваші паролі і паролі ваших співробітників надійні та захищені. Ніколи і ні з ким не діліться паролями. Використовуйте різні і довгі паролі для кожної служби, якою ви користуєтеся. Щоб допомогти вам запам'ятати їх, використовуйте програмне забезпечення для управління паролями. Крім того, найпростіший спосіб створення надійних паролів - це набір довгих фраз, які ви можете запам'ятати. Паролі із восьми символів сьогодні легко зламуються способом підбору.

У таких захищених продуктах, як Acronis Cyber Cloud або Acronis Cyber Backup, ми ніколи і ніде не зберігаємо паролі, що запобігає несанкціонованому доступу до ваших даних.

Нарешті, не забувайте блокувати свій ноутбук або настільний комп'ютер і обмежувати доступ до нього - навіть якщо ви працюєте вдома. Існує безліч випадків, коли хакери можуть вкрасти конфіденційну інформацію з незаблокованого комп'ютера, навіть перебуваючи на відстані.

Додаткові ресурси

Webinar On-demand: Cybersecurity 2021 – The Expected Threat Landscape

White Paper: Acronis Cyber Readiness Report

Free Tool: Cybersecurity Assessment Questionnaire

Acronis

Про Acronis

Acronis об'єднує захист даних і кібербезпеку, забезпечуючи автоматизований кіберзахист, який вирішує проблеми безпеки, доступності, конфіденційності, автентичності та захисту (SAPAS) сучасного цифрового світу. Завдяки гнучким моделям розгортання, що відповідають вимогам постачальників послуг та IT-фахівців, Acronis забезпечує чудовий кіберзахист даних, додатків і систем за допомогою інноваційних антивірусних рішень нового покоління, рішень для резервного копіювання, аварійного відновлення та управління захистом кінцевих точок. Завдяки зазначеним нагородами технологій захисту від шкідливих програм на основі штучного інтелекту і аутентифікації даних на основі блокчейна Acronis забезпечує захист будь-якого середовища - від хмарного до гібридного і локального - за низькою і передбачуваною ціною.
Заснована в Сінгапурі в 2003 році і зареєстрована в Швейцарії в 2008 році, компанія Acronis сьогодні налічує понад 1500 співробітників в 33 офісах в 18 країнах. Її рішенням довіряють більш 5,5 мільйона домашніх користувачів і 500 000 компаній, включаючи 100% зі списку Fortune 1000, а також професійні спортивні команди найвищого рівня.

Залишились питання?
Зв'яжіться з нами зручним для вас способом: info@softico.ua | +380 44 383 4410