



СЕРГІЙ БОБРОВ,
начальник відділу розробки
системних рішень
«ЕС ЕНД Т1 УКРАЇНА»

«ЕС ЕНД Т1 УКРАЇНА» – компанія-інтегратор телекомунікаційних і корпоративних інформаційних систем, що працює на ринку України з 1993 року. Є частиною міжнародної корпорації S&T AG, яка веде свою діяльність у більш ніж 25 країнах світу, зокрема є провідним постачальником послуг консалтингу, аутсорсингу і системної інтеграції, а також IT-послуг у Центральній і Східній Європі.

– Інформаційна безпека і кібербезпека: в чому відмінність?

– Термін «кібербезпека» описує комплекс заходів для запобігання кібератакам на інформаційну систему компанії або зниження шкідливого впливу від уже здійснених атак. Термін «інформаційна безпека» охоплює значно ширше коло питань, а саме захист інформації від витоку, втрати або її недоступності внаслідок різних факторів, зокрема не пов'язаних з кібератаками.

– Які основні ризики безпеки великих даних у компаніях same аграрного напряму Ви можете назвати?

– По суті, захист великих даних нічим не відрізняється від захисту будь-яких інших даних. Однак втрата великих даних (приміром, картографічних або статистичних в агрокомпаніях) буде неправильною, адже без них вже не можна буде виконати ефективний аналіз. А їх повторний збір потребуватиме і часу, і великих витрат.

Якщо ризик витоку даних, який пов'язаний з несанкціонованим поширенням внутрішньої інформації та аналітичних алгоритмів, в перспективі може дати деяку перевагу менш «просунутому» конкуренту, то знищення даних гарантовано призведе до прямих фінансових втрат і/або зниження ефективності інформаційної та аналітичної підсистем компанії через втрату інформаційного масиву для обробки.

– З яких елементів має складатися комплексна система кібербезпеки в аграрній компанії?

– Мобільність співробітників, IoT і «хмарне» зберігання інформації є новими викликами для кібербезпеки підприємства, що вимагає нових підходів і нових парадигм безпеки.

На сьогодні до класичної базової моделі безпеки (міжмережевий екран наступного покоління та системи антивірусного захисту) додалися системи безпеки робочих місць і мобільних пристрійів співробітників поза периметром компанії, а також системи безпеки даних, які зберігаються або обробляються поза компанією – у «хмарі». Крім того, дедалі більшу популярність здобувають системи контролю доступу до мережі для рядових користувачів і системи контролю доступу до інформаційних систем і дій для «суперкористувачів». Ще одним компонентом сучасних систем кібербезпеки є системи штучного інтелекту, які надають

можливість аналізувати зашифрований трафік та особливості мережевої активності і поведінки користувачів.

З точки зору зміни парадигми безпеки сучасні CISO/CIO визнають, що захист периметра не може гарантувати стовідсотковий захист від проникнення, тому не дуже доцільно витрачати більшість ресурсів на модернізацію його захисту, ігноруючи при цьому системи контролю процесів і дій зловмисників всередині периметра мережі. Тому компанії сьогодні приділяють дедалі більшу увагу аналізу подій, мережевої поведінки і поведінки користувачів, загалом побудові системи реагування на загрози безпекі (CERT або SOC).

Такі системи дозволяють «побачити» сотні тисяч подій у мережі і в результаті їх обробки та кореляції надати команді кібербезпеки перелік виявленіх проблем, оформленіх у вигляді інцидентів для аналізу і розслідування командою SOC на базі політик, які адаптовані для кожного підприємства. Така побудова системи безпеки надає можливість боротися з атаками, які не локалізували системи безпеки периметра й антивіруси, але виявили системи SOC на основі активності в мережі.

Якщо ж відповісти на це питання з позиції стратегії компанії, то елементами комплексної системи кібербезпеки є насамперед команда, налагоджені процедури роботи, технічні засоби. Саме в такій послідовності...

– Чи має система кібербезпеки якісні особливості залежно від масштабу бізнесу?

– Звичайно, масштаб підприємства впливає на систему інформаційної та кібербезпеки. Насамперед через те, що велике підприємство має складнішу структуру обробки даних і накопичує більше інформації, втрати або витік якої призведе до більших втрат. До того ж більше підприємство може інвестувати в безпеку більше коштів, що, крім потужніших систем безпеки, дає змогу впроваджувати спеціалізовані системи, спрямовані на захист IT-рішень, які в невеликих компаніях просто відсутні (віддалені офіси і працівники, БД, службові сервери



тощо), і ті рішення, впроваджувати які в невеликих компаніях може бути невигідно (DLP, PAM). Питання рівня доцільності певних інвестицій можна розглядати за аналогією з логікою виробників сейфів: «Захиститися від зламу неможливо, але ми можемо зробити так, щоб ціна зламу була вищою, ніж ціна того, що знаходитьться в сейфі».

– Новим трендом в агробізнесі є хмарне зберігання інформації. Які особливості захисту таких даних?

– Використання ресурсів зовнішніх центрів обробки даних (це і аналітика в «хмарі», і зберігання даних, і SaaS) – це необхідність, хочуть цього CISO чи ні. Бізнес використовує «хмари» тому, що це вигідно, зручно або тому, що іноді це єдиний варіант отримати послугу, і службі безпеки необхідно забезпечити безпеку таких комунікацій. Для цього використовуються системи класу CASB (Cloud Access Security Broker), які покликані забезпечити контроль та управління доступом до мережі й інформаційних ресурсів, антивірусний контроль (і його більш комплексний варіант – Endpoint protection), захист периметра та управління мобільними пристроями, а у разі хмарного зберігання – ще й контроль і управління безпекою в «хмарі» (CASB).

Водночас захист від знищенння даних повинен бути частиною комплексної політики безперервності бізнесу (BCP) і ґрунтуються насамперед на плані відновлення після катастрофи (DRP). Звичайно, ми не можемо гарантувати, що дані в жодному разі не будуть знищені через, приміром, техногенну катастрофу або супер-атаку, але ми повинні зробити все, щоб можна було відновити дані в задані строки і з заданим рівнем актуальності. Тому особливу увагу слід приділити розробці та впровадженню процесу резервного копіювання і відновлення (PKiB). При цьому недостатньо просто придбати програмно-апаратний комплекс і налаштувати його, необхідно приділяти увагу перевірці резервних копій на консистентність та забезпечити географічне рознесення місць зберігання копій. До того ж великий обсяг геопросторових даних потребує

“
Використання ресурсів зовнішніх центрів обробки даних (це і аналітика в «хмарі», і зберігання даних, і SaaS) – це необхідність, хочуть цього CISO чи ні

більше продуктивних каналів і сховищ, а також більш швидкісних каналів, звичайно, з урахуванням вартості інформації, захист якої потрібно забезпечити. Завдання системних інтерegratorів – описати, навіщо і як це зробити. І лише власнику даних визначати, готовий він інвестувати у збереження своєї інформації чи ні.

– Як захистити дані своїх співробітників?

– Дані співробітників, як і інші корпоративні дані, необхідно зберігати у корпоративній інфраструктурі, що забезпечує контроль доступу та захист від втрати. Узагалі дані співробітників, які зберігаються на персональних пристроях, – це потенційна «жертва» розкрадання, втрати та ураження вірусами. Тому, якщо дані все ж повинні бути на кінцевих пристроях, то рекомендується самі кінцеві пристрої «перенести на сервер» – віртуалізувати кінцевий пристрій на базі VDI або RDP. І хоч віртуалізація робочих місць майже ніколи не приносить прямого економічного ефекту, але вона завжди забезпечує підвищення керованості, збереження даних і безпеку.

– Система кібербезпеки майбутнього. Якою вона може бути?

– На мою думку, збережеться та посилються тенденції до контролю та аналізу процесів всередині мережі та інформаційної інфраструктури. Також можна передбачити, що системи безпеки будуть будуватися на базі систем аналізу поведінки із залученням штучного інтелекту, який аналізуватиме величезний обсяг подій від різних систем для формування загальної картини всіх процесів інформаційної інфраструктури.