CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 03.12.2020 г.

Съдържание

4 правила, които премахват рисковете за сигурността при облачната миграция

Предприятията все повече преместват своите приложения в облака. Мигрирането на приложения и данни към публичния облак има много предимства, но въвежда и много предизвикателства за киберсигурността, които нарушават старите модели. Много организации не успяват да вземат предвид това прекъсване при проектирането на своите протоколи за сигурност. За да извлече напълно възможностите за производителност на облака, вашата организация трябва да преосмисли своите протоколи за киберсигурност.

Ето четири процеса, които могат да ви помогнат да се справите с изискванията на публичния облак.

Адаптирайте се към новите режими на работа

Облачните приложения изискват внедряване на динамични модели за сигурност. Вашата организация трябва да преосмисли своя DevOps цикъл и да го приведе в съответствие с най-добрите практики за сигурност. Промяната на културата около сигурността и превръщането й в ключова част е най-доброто, с което можете да започнете

Повечето разработчици нямат опит в сигурността. За тази цел прилагайте програми за съвместно обучение, които позволяват засилено взаимодействие между екипите за сигурност и развитие.

Много организации правят грешката да се опитват да изградят план за управление на събития в облака от самото начало, вместо да се възползват от опита на трети страни. По време на ранните етапи на вашия процес на миграция в облака, трябва да си сътрудничите силно с вашия доставчик на облачни услуги (CSP), за да интегрирате способностите на облака с вашите нужди.

Също така трябва да сте в течение с изискванията за съответствие и трябва да създадете план, който да бъде в крак с последните промени. Много доставчици на облачни услуги предлагат, но най-добре е да създадете свой собствен план.

Настоявайте за сигурност и поверителност, предвидени в дизайна

Старите протоколи за киберсигурност функционират като добавка към приложения и данни. Неуспехът да се преустрои тази структура води до тромав и неефективен работен процес. Управлението на самоличността е в основата на успешния протокол за обществена сигурност в облака.

Много доставчици на облачни услеги предлагат услуги за управление на самоличността с автоматизирани схеми за оторизация.

Демократизацията на данните е необходимост в наши дни, за да се реагира на бързо променящите се бизнес условия. Създайте протоколи, които ясно определят достъпа въз основа на нуждите и рисковете на служителите. Често срещана грешка, която организациите допускат, е да се предоставят разрешения за управление по подразбиране. Базирането на достъпа до ръководството може да доведе до излишни акаунти, които могат да бъдат уязвими към целенасочена атака.

Въпреки че искате да осигурите възможно най-добър достъп до данните, трябва да приемете протоколите за криптиране като стандарт. Данните, независимо дали са в покой или в движение, трябва да бъдат криптирани при източника, за разлика от криптирането, когато влизат в периметъра на вашата мрежа. Вземете решение за надежден протокол за управление на ключове. Някои компании избират да съхраняват ключове локално, докато други избират да разчитат на CSP, за да ги съхраняват.

Избраният от вас метод зависи от вашите изисквания за съответствие. Често съхраняването на ключове с CSP подобрява производителността на приложенията, тъй като те се нуждаят от ключовете за дешифриране на данни. Проведете задълбочен одит на вашите нужди и работете с вашия CSP, за да създадете протокол, който ви подхожда най-добре.

Разширете обхвата на покритието си

Докато проектирането на надеждни протоколи за вътрешна сигурност е едно, защитата на вашата мрежа и приложения от данни на доставчици на трети страни е друго. Не можете да контролирате техните протоколи за сигурност, освен да предоставяте препоръки и да се надявате, че те са приложени. И така, как можете да осигурите вашата безопасност?

Започнете, като създадете SLA, които изискват от вашите доставчици да спазват минималните стандарти за сигурност. Това е особено важно при управлението на данните, които влизат във вашата система. Определете протоколи за криптиране и проверете данните за злонамерено поведение. Използвайте разрешения и протоколи за

управление на самоличността, за да управлявате стриктно достъпа на доставчика до вашата мрежа.

Провеждайте редовни одити с вашите доставчици, за да сте сигурни, че условията за SLA се спазват през цялото време. Определете ясно периметъра на вашата мрежа. Понастоящем много организации насочват трафика през центрове за данни на място, комбинирани с VPN, за да осигурят сигурен достъп до данните в публичния облак. Сложността на тази задача обаче на практика гарантира, че в крайна сметка ще се използват контроли за периметър на трети страни.

Започнете да оценявате нуждите на вашата инфраструктура, за да поддържате тези периметърни услуги на трети страни. Може да са ви необходими множество приложения, които покриват вашите уебgateways, защитни стени и нужди от мрежово наблюдение. Преминете към непрекъснат протокол за проверка на сигурността, който редовно сканира вашата мрежа за уязвимости, вместо да разчитате само на пенетрейшън тестове.

Приемете индустриалните инициативи

Киберсигурността е бързо развиваща се област благодарение на естеството на заплахите.

Приемете инициативи в целия бранш или създайте работна група за разработване и определяне на стандарти за сигурност във вашата индустрия.

Сътрудничеството с колеги от вашия бранш е чудесен начин да се наложат стандартите за ДОУ и гарантира, че тези стандарти ще се налагат и на всички доставчици.

Облачната миграция е чудесен начин за подобряване на използваемостта на вашите приложения, но гарантирането, че остават сигурни, не е лесна задача. С тези процеси ще създадете сигурна среда за вашите служители и клиенти.

За повече информация:

https://www.cybersecurity-insiders.com/4-protocols-that-eliminate-the-security-risks-of-cloud-migration/

Как да подобрите киберсигурността на работното си място

В миналото организации със слаба киберсигурност са били жестоко наказвани с кибератаки, пробиви на данни и огромни загуби. Според Varonis и RiskBased над 4 милиарда записи са били достъпни незаконно чрез пробиви на данни през 2019 г. Тази изумителна цифра посочва защо компаниите трябва да имат стабилна холистична стратегия за киберсигурност.

Интересното е, че хората изглежда са осъзнали по-добре необходимостта от сигурно работно място през 2020 г. Nexor, доставчик на услуги в пространството за киберсигурност, твърди, че в Google се търси „киберзащита“, което е нарастване със 126% през първото тримесечие на 2020 г. и сравнено със същия период на миналата година – нарастване със 116% !

Но докато информираността е висока, действащите мерки са по-малко. По-долу ще ви преведем през най-добрите практики, които ще ви помогнат да подобрите киберсигурността на вашата компания.

Сигурност чрез VPN

Инвестирането в стабилно решение за сигурност на данните може да бъде трудно, особено за по-малки фирми с малко ресурси. В такъв случай виртуалната частна мрежа е втората най-добра алтернатива. Използването на виртуална частна мрежа на работното място създава по-сигурна връзка, чрез която служителите имат достъп до файлове.

Наред с много други предимства, VPN криптира тези файлове и поддържа онлайн активността частна, като маскира реалния IP адрес на потребителя. Ето различните начини, по които VPN повишава киберсигурността:

Шифроване

Технологията за криптиране във VPN помага да се скрият данните на потребителя. Най-добрите VPN, като ExpressVPN, предлагат най-доброто в класа AES криптиране с 256-битови ключове, стандартът, използван от правителството на САЩ. Поради сигурността, осигурена от криптирането, можете да съхранявате фирмени данни в движение от любопитните погледи на киберпрестъпниците.

MultiHop

Тази функция ви позволява да се свързвате едновременно с различни сървъри. Технологията повишава нивото на сигурност чрез прилагане на двойно криптиране.

Анти-зловреден софтуер / фишинг

Не всеки работещ е технически подготвен и може да идентифицира вредни връзки. Опцията за анти-злонамерен софтуер и анти-фишинг в някои VPN се удвоява чрез прихващане на фишинг атаки, изскачащи реклами и други злонамерени кибер заплахи. С тази опция фирмените данни могат да бъдат защитени, като се избягват злонамерени връзки.

Множество протоколи за сигурност

VPN също се предлагат с широк спектър от протоколи за сигурност. Стандартният протокол е OpenVPN и е силно препоръчителен поради страхотния си баланс между скорост и сигурност. Има обаче и други защитени протоколи, които можете да използвате, като IKEv2.

Wi-Fi криптиране

Криптирането на Wi-Fi връзката на вашето работно място допринася много за подобряването на цялостната киберсигурност. Можете да започнете с най-основната мярка за промяна на паролата на рутера на по-силна, преди да преминете към предварителни опции, които включват конфигурация на рутера. Имайте предвид, че под парола на рутера имаме предвид паролата, която защитава вашата Wi-Fi конфигурация, а не тази, която позволява достъп до мрежата.

Мениджъри на пароли и двуфакторно удостоверяване

Паролите отдавна са отлични методи за идентичност и контрол на достъпа. Надеждността им обаче често зависи от това как те се използват в рамките на организацията. Ще се изненадате, че повечето служители използват прости пароли или по-лошо, една и съща парола за различни акаунти, страхувайки се да не забравят комбинациите.

Тази практика излага данните на компанията на пробиви, тъй като хакерите могат лесно да разбият паролите. За по-добра сигурност на паролата е силно препоръчително да използвате мениджър на пароли. Това е удобен помощен инструмент, който поддържа вашите пароли сигурно и гарантира, че използвате силни пароли по всяко време. Мениджърите на пароли също позволяват на членовете, използващи един и същ акаунт, да споделят безопасно пароли.

Двуфакторното удостоверяване (2FA) също трябва да се използва, защото затруднява киберпрестъпниците да получат нелегален достъп до акаунти на персонала. Имайте предвид, че 2FA не е задължително да се основававърху кодове и цифри. Служителите могат алтернативно да използват приложения като Google Authenticator, които препращат известия за одобрение на мобилни устройства.

За повече информация:

https://www.cybersecurity-insiders.com/how-to-improve-your-workplaces-cybersecurity/