CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 04.12.2020 г.

Съдържание

5 задачи, които индустрията в областта на киберсигурността трябва да реши през 2021 г.

С изтичането на 2020 г. специалисти по киберсигурност по целия свят започнаха да оценяват как да направят най-значимите подобрения през следващата година.

Ето пет въпроса, които секторът на сигурността трябва силно да обмисли, да предприеме колективен подход за поправяне - или поне за подобряване - през 2021 г.

1. Хората, които са зле оборудвани да работят от вкъщи

Пандемията COVID-19 накара много хора, вземащи решения, да позволят на хората да работят от вкъщи, когато е възможно. Всъщност служителите на много компании ще продължат да го правят в обозримо бъдеще. Въпреки това отдалечените работни среди въвеждат нови проблеми със сигурността.

Проучване на IBM, проведено през юни 2020 г., разкри някои тревожни констатации. Например 45% от служителите не са били обучени, преди да започнат да работят дистанционно. Тогава 53% съобщиха, че използват лични лаптопи, без да ползват нови инструменти за сигурност за тези устройства.

Специалистите в областта на ИТ сигурността не могат да приемат, че служителите знаят как да се пазят онлайн, докато работят от вкъщи. Предоставянето на широко достъпни инструменти като мениджъри на пароли и разпространение на контролни списъци за киберсигурност с най-добри практики може да помогне на организациите с разпределена работна сила да поддържат защита от заплахи.

2. Рансъмуерът нараства в световен мащаб

Ransomware е проблем, който няма да изчезне скоро. Проблемът е, че се влошава. Фирмените лидери трябва да се подготвят сега, за да го ограничат в бъдеще.

Изследвания, свързани с третото тримесечие на 2020 г., установяват 98,1% увеличение на атаките на рансъмуер в САЩ в сравнение с данните от първото тримесечие. Двойното изнудване е друга скорошна тенденция. Преди киберпрестъпниците да криптират откраднатa информация, те вземат поверителни данни и заплашват да ги публикуват, освен ако жертвите не платят исканата сума.

Извършването на редовни архиви на данни и осигуряването на достъп до съдържанието чрез няколко метода може да позволи на компаниите да продължат да работят гладко, ако нападателите посегнат върху важни файлове. Въпреки това специалистите по сигурността трябва да положат по-големи усилия, за да идентифицират и отстранят уязвимостите, които дават достъп на неупълномощени страни до техните ресурси.

3. Липсата на разделение между половете

Проучване, свързано с центрове за данни, установи, че жените обикновено заемат по-малко от 5% от ролите на персонала в тези съоръжения. Това е реалността, въпреки същото проучване, което показва, че 45% от анкетираните смятат, че липсата на женско представителство представлява заплаха за техния отрасъл.

За съжаление ситуацията не е много по-добра в сектора на киберсигурността. Статистиката показва, че жените съставляват само 14% от работната сила в Северна Америка по киберсигурност, едва 7% в Европа и 5% в Близкия изток.

Компаниите могат да се справят с този проблем по много начини. Например, те могат да стартират програми за стипендии или възможности за стаж, които са специално насочени към жените в киберсигурността.

4. Грешно възприемане на индустрията за киберсигурност и нейните специалисти

Индустрията за ИТ сигурност има проблем с културата.

Широкото обществено схващане е, че киберсигурността е специалност на „тъмните изкуства“, пълна с мистика. Това предположение често насърчава разработването на инструменти за ИТ сигурност, които са прекалено сложни и плашещи за обществото.

Професионалистите по киберсигурност притежават специализирани умения, но те трябва да играят централна роля в разпространението на идеята, че всеки може да помогне за сигурността на нашата инфраструктура.

5. Загриженост относно безопасността в помещенията

Докато много служители могат да работят от вкъщи, за да останат в безопасност по време на пандемията, специалистите по киберсигурност често нямат тази възможност. Някои изпълняват задължения, които изискват влизане в офиси. Други работят в класифицирани съоръжения, които не позволяват отдалечени възможности.

За съжаление 78% от професионалистите в сферата на киберсигурността съобщават, че имат притеснения относно своята безопасност, докато са на място. Организационните лидери не могат да премахнат всички рискове, но могат да ги минимизират.

Предоставянето на маски и дезинфектант за ръце за персонала на място са добри отправни точки. Вземащите решения обаче също трябва да изследват стъпкови смени и хората да работят последователно заедно със същите колеги. Тези неща намаляват времето, което служителите прекарват с по-голям брой хора, ограничавайки потенциала за предаване на вируси и улеснявайки по-доброто проследяване на контактите, ако се появи огнище на зараза.

За повече информация:

https://www.cybersecurity-insiders.com/5-issues-the-security-industry-needs-to-resolve-in-2021/

Как да стартирате одит за киберсигурност във вашия бизнес

Хакер атакува на всеки 39 секунди. Това сочи проучване, проведено от университета в Мериленд. Hackerpocalypse изчислява, че киберпрестъпността ще струва на глобалния бизнес най-малко 6 трилиона долара до 2021 г. Хакерите продават идентификационни данни на акаунти, поверителна финансова информация и чувствителни данни. Най-малко 16 милиарда записи са били изложени на киберпрестъпници и според проучването това е с 273 процента повече в сравнение с данните от миналата година.

Тези статистически данни показват, че повечето мерки, предприети от експерти по киберсигурност, не работят. Намаляването на такива рискове изисква ефективни стратегии за киберзащита и контрол на сигурността. За съжаление защитата на защитната стена и антивирусният софтуер изглеждат неадекватни мерки за противодействие на пробивите. За ефективното намаляване на тези цифри е необходима радикална промяна в мисленето.

Предприятията трябва да извършват самоодити и да се позиционират по начин, който се противопоставя на нарушаването на данни. Киберпрестъпността е разочароваща и плашеща за всички участници в индустрията, включително потребителите, малкия и големия бизнес. Ето защо една компания трябва да предприеме подходящи стъпки за провеждане на успешен одит на киберсигурността.

Определете приоритетите си

Общият регламент за защита на данните изисква фирмите да имат служител по защита на данните. Този служител отговаря за проследяването на всички данни, които влизат и излизат от бизнеса. Освен това служителят отговаря и за провеждането на вътрешен одит на сигурността. Най-добрият контролен списък изброява всички активи, за да се определи до какви граници ще се простира одитът. Тези активи могат да бъдат компютърно оборудване, данни за клиенти, информация за компанията и чувствителна бизнес информация. Активите включват и всичко, в което компанията влага време, пари и ресурси за успешното управление на бизнеса. Например комуникационни системи и вътрешна документация.

Какви са потенциалните заплахи

Това може да са слаби пароли, несигурна инфраструктура, данни за фирми и клиенти. Повечето биха могли да мислят, че атака за отказ от услуга ще се осъществи само виртуално. Това е невярно, тъй като физическо нарушение като пожар също може да доведе до отказ от услуги. Понякога дори природни бедствия като наводнения могат да причинят такива атаки. Затова имайте предвид всяка възможна заплаха, пред която е изправен бизнесът. Обмислете следния списък с чести заплахи за сигурността:

- Фишинг атаки - Повечето фишинг атаки са мотивирани от необходимостта от финансови перспективи. Експертите по фишинг обикновено се насочват към чувствителна информация, която ще им позволи да организират последователни атаки за кражба на пари или продажба на важна информация.
- Слаби пароли - При поне 81 процента от пробивите през 2017 г. хакерите се възползваха от слабите пароли. Обикновено слабите пароли са първата стъпка, предприета от хакерите за използване на системите.
- Вътрешни заплахи - Понякога престъпникът не е далеч. Помислете за някой в бизнеса, който се опитва да навреди на бизнеса. Това също може да е случайно нарушение отвътре. Въпреки това, злонамерени или случайни, предприятията трябва да вземат предвид всеки възможен риск.
- DDoS - Разпределени атаки за отказ от услуга възникват, след като стекове от системи нахлуват в дадена цел и я претоварват. Например уеб или мрежов сървър. Това действие прави сървъра безполезен и го отваря за атака.

- Устройства за служители - Абонаментът на устройства за служители за Wi-Fi на бизнеса може значително да отслаби предимството ви за сигурност.
- Зловреден софтуер - Това са всички заплахи като троянски коне, червеи или шпионски софтуер. Днес глобалният бизнес е изправен пред неочакван прилив на инциденти с рансъмуер.
- Стихийно бедствие / Физическа кражба - Подгответе се за природни бедствия или физическа кражба.

Оценете съществуващия процес на сигурност

След като осъществите достъп до потенциални заплахи за сигурността, преценете дали настоящата инфраструктура на вашия бизнес е достатъчно солидна, за да се противопостави на пробив. Оценете ефективността на настоящите мерки и идентифицирайте всички потенциални слабости. Вземете предвид целия бизнес, включително персонала и процедурите за сигурност. Може да помислите за външен одит за тази стъпка. Това обаче не е задължително. Независимо от това, вътрешните пристрастия могат да изкривят резултатите от одита по време на този процес.

Приоритизирайте

Преоценете потенциалната заплаха, определете шансовете за всяка заплаха, която се случва и дайте на всяка заплаха оценка на риска. По време на този процес проучете следното:

1. Бизнес историята на кибер пробивите - изправял ли е бизнесът пред атака?
2. Тенденции в киберпрестъпността - Какви методи използват днешните киберпрестъпници, за да атакуват бизнеса. Какви заплахи са по-разпространени от други и кои са по-малко вероятно да се случат.
3. Тенденции в индустрията - Бизнесът във финансовия сектор е по-вероятно да се сблъска с изтичане на данни, отколкото други индустрии.
4. Регламенти, изисквания и законодателство - Помислете кой има достъп до вашите най-чувствителни данни. Вземете под внимание дали вашият бизнес е частна или публична организация. Идентифицирането на хората, които имат достъп до вашите данни, помага да се определи точният рейтинг на заплахата за определени области.

И накрая, избройте всички потенциални заплахи срещу техните рискови оценки.

Финализиране на оценката

Завършете одита, като изготвите набор от протоколи за сигурност за елиминиране на риска. Те включват:

Създаване на сесии за обучение на служители за генериране на информираност за съществуващите кибер заплахи.

1. Защитата на имейла е необходима чрез прилагане на мерки като спам филтри.
2. Необходими са редовни архиви, за да се поддържа бизнесът в случай на компрометиране.
3. Актуализиран софтуер, за да гарантирате, че вашият набор от инфраструктура е на ниво с отрасловите стандарти.
4. Управление на пароли, което създава уникални и сложни пароли.
5. Софтуер за мрежово наблюдение, за да ви предупреди в случай на подозрителна дейност.

В заключение, създайте бизнес култура във вашата компания, където всеки човек разбира всяка потенциална заплаха за сигурността.

За повече информация:

https://www.cybersecurity-insiders.com/how-to-run-a-cybersecurity-audit-at-your-business/