ISSN 2738-7089 https://doi.org/10.11610/cybsec03bg

British Embassy Sofia

Информационен бюлетин за киберсигурност

ИИКТ
Институт по информационни и комуникационни технологии

Британско-Българско партньорство в киберсигурността за МСП и организации

Бюлетин Ноември 2020 Номер 3

Цели и обхват

Съдържание:

Настоящият онлайн бюлетин е фокусиран върху предизвикателствата, свързани със защитата на домашните мрежи на служителите и как интелигентните устройства променят модела на заплаха, свързан със споделянето на данни. В следствие от кризата с COVID-19, екипите за сигурност и ИТ са ангажирани в дейностите по подпомагане и защитаване на служителите, които трябва да работят отдалечено.

В броя са представени са практически препоръки от експерти по сигурността за намаляване на рисковете за корпоративната сигурност, предизвикани от домашните мрежи и устройствата, поддържащи т. нар. интелигентен дом. Експертите по сигурността дават осем практически препоръки за защита на служителите, работещите от разстояние. В тази вразка е необходима строга политика за всички служители работещи от вкъщи, която задължително включва използването на антивирусен софтуер при достъп до ресурсите на организацията. Следва да се обмисли и прилагането на алтернативни облачно-базирани инструменти за наблюдение на работните станции. Необходимо е да се направи анализ на поддържаните конзолни инструменти и лицензите за достъп до компютри извън домейна. Едно добро решение е използването на инструменти като Splashtop SOS или LogmeinRescue, за да се позволи на екипа за ИТ поддръжка да осъществява дистанционен достъп до домашните машини на служителите, като по този начин може да се окаже съдействие при настройването на отдалечения достъп до ресурсите на организацията.

В настоящия брой е представена компанията CounterCraft, която е пионер в предоставянето на продукти срещу кибер измама и за контраразузнаване, подпомагащи откриването на целенасочени атаки. Решението на CounterCraft открива базирани на измама кампании и предлага детайлен мониторинг и комплексни действия за реакция. Платформата, откриваща кибер измами се използва от правителствените правоприлагащи органи.

Дадена е полезна информация за проблемите на сигурността, при работа от разстояние, чрез предоставените безплатни електронни книги и инструменти за киберсигурност, които ще помогнат за защита и управление на работещите от вкъщи. Съвети за сигурността на отдалечената работна сила и най-добри практики от професионалисти по сигурността, също могат да бъдат намерени. И накрая, дадени са допълнителни препоръки, новини и статистики относно дистанционната работа от вкъщи. Представен е и списък с връзки към български, британски и международни кибер-институции.

Редактори на броя: **проф. д.н. Даниела Борисова**
докторант Зорница Димитрова

Фокус на изданието: Предизвикателства при защитата на домашните мрежи на служителите и как интелигентните устройства променят модела на заплаха, свързан със споделянето на данните

проф. д.н. Даниела Борисова, ГИМ, ИИКТ-БАН

Зорница Димитрова, докторант в ИИКТ-БАН

Дистанционната работа не е ново предизвикателство. Много компании и преди се възползваха от отдалечена работа, за да дадат на служителите си по-добър баланс между работа и личен живот, а това от друга страна допринася и за намаляване на въглеродния отпечатък и повишаване на ефективността на бизнеса. Поради пандемичната обстановка, предезвикана от COVID-19, в световен мащаб работата от разстояние се превърна в необходимост за съвременните организации, които трябва да създадат планове за непрекъснатост на бизнеса. Това е свързано с много ИТ предизвикателства за служителите, работещи от вкъщи.

От ИТ гледна точка има много неизвестни, свързани с управлението на отдалечената работа:

- Домашните Wi-Fi мрежи и рутери се компрометират по-лесно от индустриалното оборудване в офисите, което увеличава риска от излагане и неволно изтичане на корпоративни и клиентски данни.
- Все повече данни се съхраняват в облака и този основен елемент трябва да бъде правилно защитен, като се използват подходящи стратегии.
- Корпоративните VPN мрежи рядко са достатъчно скалируеми, за да отговорят на нарастването на служителите с отдалечен достъп до мрежата. Това може да повлияе на производителността, което допълнително усложнява защитата на данните.
- Обменът на имейли се увеличава, а липсата на разграничение на личните комуникации, допринася за увеличаване на вероятността електронната поща да съдържа чувствителна информация заедно с потенциални лични данни.
- Широкото използване на инструменти за видеоконференции ще доведе до намаляване на честотната лента в много региони, така че хората ще разчитат на комуникация по имейл в пиковите часове.

От удобството на домашния си офис служителите може да не вземат достатъчно предпазни мерки, като например да използват само корпоративна електронна поща. Вместо това те могат да изпратят работни файлове по личния си имейл, за да свършат работата по-бързо – практика, която излага корпоративната информация на риск.

VPN трябва да се използва за приложения, изискващи отдалечен достъп. VPN мрежите осигуряват гъвкава връзка с различни услуги (уеб страници, е-мейл, SQL сървър и др.) и могат да защитят трафика. Трябва да се вземе предвид, че не всички VPN услуги си струват парите, поради това е добре да се оценят някои задължителни неща, преди да се избере VPN технология. VPN услугите, използвани за целите на поверителността, защитават само данните от и до VPN доставчика, а не до местоназначението, така че не са подходящи за защита на отдалечен достъп. В някои случаи е възможно също така да се настроят криптирани отдалечени връзки чрез Remote Desktop или друг подобен сървър. Много от тези видове връзки (RDP, HTTPS, SSH) включват криптирането като

част от услугата и не изискват допълнителна VPN или друга криптографска технология, за да осигурят данните при преминаване.

Нуждата от политика за сигурност на дистанционната работата е всеобща и належаща. Организациите трябва да разработят политика за отдалечена работа, за да информират редовно служителите какво се очаква от тях, когато работят от вкъщи. Например добра практика е да се предоставя достъп до корпоративни ресурси само на служителите, които използват бизнес имейл акаунти, и да се блокират всички останали. Същото се отнася и за използването на системи за видеоконференции при организиране на семинари, лекции, тестове и други. Приложимостта на това правило е доказана в практиката на провежданите лекции и тестове през последните 2 семестъра в Университета по библиотечни и информационни технологии. За съжаление, някои организации с недостатъчно ниво на компетентност позволяват използването на лични имейл адреси за бизнес кореспонденция. Потребителите, работещи от дома, трябва да са наясно с рисковете в домашната мрежа и трябва да бъдат обучени от организациите как да ги сведат до минимум. В тази връзка, по време на конференцията **DIGILIENCE'2020** на 1 октомври 2020 беше проведена кръгла маса с акцент върху ролята и отговорностите на главния информационен мениджър (ГИМ). Наред с отговорностите на ГИМ, беше отделено и необходимото внимание на ролята на ГМИС (главния мениджър по информационна сигурност), на който основното задължение е да гарантира сигурността на информацията и данните. В допълнение към важната роля на ГИМ и ГМИС, на 18 януари 2021 г. се планира онлайн курс за обучение на CIO/CDO. Лектор ще бъде проф. Сирадж Шайк – професор по системна сигурност в Института за транспорт и градове на бъдещето, Университет Ковънтри (Великобритания).

Осем практически препоръки за кибер защита на служителите в условията на отдалечена работа

8 ключови съображения за защита на работещите отдалечено
(източник: csoonline.com)

Много служители по света са принудени да работят от вкъщи поради свързаните с COVID-19 правила за социално дистанциране. Според анализаторите, тази тенденция засилва необходимостта организациите да обръщат повече внимание на сигурността на домашните мрежи и на продуктите за интелигентен дом и други устройства, свързани с тях. Домашните рутери, принтери, системи за сигурност, DVRs, игрови конзоли и други интелигентни устройства могат значително да променят модела на заплахата за корпоративната мрежа.

Много екипи за сигурност и ИТ неочаквано трябва да подкрепят и защитят много на брой служителите, които трябва да работят отдалечено поради COVID-19 кризата. Ето някои области, които трябва да бъдат обхванати:

1. Определете каква защита на отдалечената машина ще ви е необходима за домашни потребители. Въпреки че може да имате конзолен достъп и възможност за управление на всички работни станции във физическия офис, вероятно нямате същото ниво за контрол на домашните компютри. Windows Defender, включен в Windows 10, е повече от приемлив антивирусен инструмент за отдалечената машина. Въпреки това всеки отдалечен работник, който има Mac OS, не трябва да

бъде освободен от използването на софтуер за защита. Един от всеки десет потребители на Mac OS е бил атакуван от **Shlayer Trojan**.

2. Преразгледайте какъв софтуер е необходим на работещите отдалечено служители. За ползващите **Office 365** има лицензи, които позволяват офис пакета да се инсталира на до пет компютъра с Windows или Mac OS, пет таблета и пет смартфона. С тези пакетни лицензи може да позволите на вашите служители да използват **Office 365 на домашните си компютри**. Може да се наложи да прегледате какви са опциите и алтернативите за лицензиране въз основа на това за коя платформа и версия на MS Office сте лицензирани в момента.

3. Уверете се, че отдалеченият достъп не създава допълнителен риск. Може да се наложи неочаквано да настройвате и лицензирате сървъри за отдалечен достъп, виртуални машини с Windows 10 или други технологии за отдалечен достъп. Не въвеждайте излишен риск по отношение на лицензите и сигурността въз основа на неточни решения. За отдалечена работа, която включва услуги за отдалечен достъп, не забравяйте, че атакуващите чрез Ransomware търсят и сканират за **отворени RDP сървъри**, насочвайки се към всеки, отговарящ на порт 3389. Не преместваите RDP на друг порт, тъй като TSgrinder сканира за RDP отговор на всеки порт.

4. Внедрете двуфакторна автентикация (2FA). Когато добавяте нови решения за отдалечен достъп, помислете за включване на **2FA**. Лесно може да се добави 2FA дори и към съществуващите локални решения за отдалечен достъп, като се използват инструменти подобни на DUO.com, който може да добави 2FA към RDGateway и Remote Web Access. Въпреки че може да се наложи на вашата организация да въведе бързо модела за отдалечена работа на служителите, все пак можете да се гарантира, че достъп до системите имат администратори и потребители, но не и нападатели.

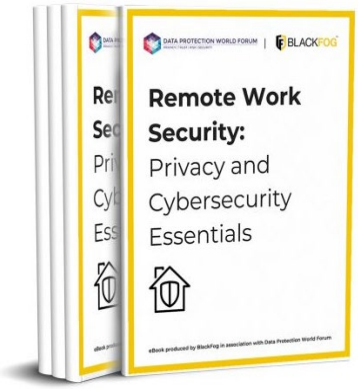
5. Използвайте виртуална частна мрежа (VPN). Напоследък има няколко **високорискови уязвимости** в VPN софтуера. Често на клиентски работни станции, които не са актуализирани от години, е оставена по-стара версия на VPN софтуера. Уверете се, че вашите VPN решения са актуални както на сървъра, така и на защитната стена, която предоставя VPN решения, а също и на работните компютри на отдалечените потребители.

6. Оценете въздействието от отдалечената работа върху защитните стени, политиките за условен достъп и журналите. Вашата организация може да има решение за регистриране на информация за сигурността и управление на събитията (**SIEM**), което преглежда трафика, идващ от локалните компютри и лаптопи към сървърни ресурси. Ако целият трафик на служителите внезапно започне да идва от различни IP адреси, данните на вашата платформа за мониторинг вече няма да бъдат „нормални".

7. Обучавайте служителите за измами свързани с COVID-19. Националната система за кибер информираност на САЩ предупреждава за циркулиращи **измами свързани с COVID-19**. Предупредете служителите си да не отварят непоискани и неочаквани имейли и да използват само официални уебсайтове. Уверете се, че организацията има централен онлайн бюлетин, предназначен за официална комуникация и уведомяване, особено в случай, че някой във вашата организация се зарази със зловреден софтуер.

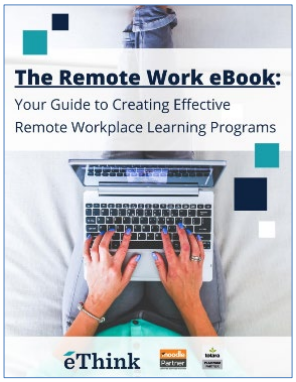
8. Актуализирайте правилата за приемливо използване на ресурсите на организацията от служителите. Уверете се, че въведените правила за използване на компютър покриват и домашните компютри, които се използват за отдалечена работа. Ако тази политика все още не е налична, ще трябва бързо да ускорите изготвянето ѝ, като позволите личните активи на служителите да се използват за отдалечен достъп до организационните ресурси. Ще трябва да работите с адвокатите и данъчните съветници на организацията, за да проверите дали използването на персонални компютри и лични телефони на служителите налага необходимост от възстановяване на разходите за използване.

Полезни електронни книги и инструменти за сигурна отдалечена работа



eBook: Remote Work Security – Privacy and Cybersecurity Essentials

The Remote Work eBook: Your Guide to Creating Effective Remote Workplace Learning Programs



Remote Working Successfully – EBook. Implement and Perfect your Remote Working Setup

CYBER SECURITY INCIDENT MANAGEMENT GUIDE

Managing Remote Workers: Free Toolkit

Следните безплатни инструменти за кибер сигурност ще помогнат за защита и управление на работещите от вкъщи:

- Безплатни инструменти за: Служители и изпълнители, работещи от разстояние;
- Безплатни инструменти за: ИТ специалисти, достъпващи привилегировани акаунти от разстояние;
- Безплатни инструменти за: ИТ специалисти, повишаващи сигурността на отдалечените работни станции.

	Remote Workforce Security Tips & Best Practices – 18 професионалисти по сигурността споделят своите най-добри съвети и практики за повишаване на сигурността при отдалечена работа.

Избрани новини и съвети за кибер защита при работата от вкъщи

Инфраструктурата на отдалеченото работно място е определена като един от десетте най-големи технологични рискове за 2021 година	Ежегодното глобално проучване на ISACA и Protiviti, което се провежда сред ИТ лидери и професионалисти, идентифицира десетте най-големи технологични рискове и предизвикателства за организациите през 2021 г. На девето място като заплаха се нарежда проблема с отдалеченото работното място. На организациите липсват достатъчно инструменти, технологии и ресурси, които да позволят и поддържат защитена отдалечена работна сила за продължителен период с необходимите нива на контрол. **ISACA and Protiviti risk survey report ...**
SASE може да засили сигурността на работещите отдалечено	COVID-19 пандемията ускори плановете на някои компании да приложат нововъзникваща концепция за киберсигурност SASE – „Услуга за сигурен достъп". Gartner въведе термина SASE, за да опише технологична категория, която обединява мрежови и защитни услуги, включително SD-WAN, защитен уеб гейтуей (SWG), брокер за защита на облачния достъп (CASB), DNS защита и облачни защитни стени. За новите потребители на SASE, обикновено най-голямото забавяне се предизвиква от страна на хардуера. Служителите може да се нуждаят от нови SASE edge устройства, за да осигуряват работа в мрежата и сигурност в домовете на служителите, но има и начини за внедряване на SASE без никакъв нов хардуер. CloudCheckr, софтуерна компания, която произвежда инструменти за управление на облак, използва платформата SASE на Zscaler, за да свърже служителите си с облачните услуги, които са им необходими, за да осъществяват работата си по сигурен начин, включително инфраструктурата на AWS. **NetworkWorld/Gartner report ...**
Кутията на Пандора за киберсигурността. Как отдалечената работа създава рискове за сигурността на организациите	Преходът към модела на отдалечена работа на фона на COVID-19 отвори кутията на Пандора за киберсигурността, с проявяващи се пропуски в сигурността и спазването на правилата, проправяйки път за потенциално компрометиране на данните. Например, проучването на SailPoint показва, че 1 от 3 служители в САЩ (33%) използват собствени лични устройства за работа от разстояние. Това е значителна разлика в сравнение с Европа, Близкия Изток, Азия (EMEA) и Австралия и Нова Зеландия (ANZ), където половината от служителите съобщават, че отдалечената работа се извършва с доставена от работодател техника. Над половината от анкетираните в EMEA и ANZ (51%) са претърпели фишинг атака от началото на пандемията. **SailPoint report ...**
Съвети за онлайн сигурност при работа от вкъщи по време на пандемията COVID-19	Някога работата от вкъщи беше лукс. Сега това се превърна в необходимост за служителите. Ето първите десет неща, с които трябва да сте наясно, за да сте сигурни, че вие и вашите служители се придържате към разумна политика за сигурна работа от вкъщи: 1) Инвестирайте в цялостен антивирусен софтуер; 2) Дръжте членовете на семейството далеч от работните устройства; 3) Инвестирайте в плъзгащ се капак на уеб камера; 4) Уверете се, че VPN на вашата

компания е възможно най-сигурен; 5) Използвайте централизирано решение за съхранение на данни; 6) Защитете домашната си безжична мрежа; 7) Бъдете наясно с рисковете за сигурността на видеоконференциите; 8) Уверете се, че паролите ви са надеждни и сигурни; 9) Максимизирайте сигурността около онлайн банкирането; 10) Обърнете внимание на сигурността на имейлите.

Kaspersky report ...

Кибер институции в изданието

CounterCraft

CounterCraft е иновативен доставчик на продукти, за противодействие на кибер измами, контраразузнаване и за откриване на целенасочени атаки. Кибер нападателите са технологично напреднали и целенасочените им атаки заплашват ежедневно големи организации. CounterCraft предоставя разпределена платформа срещу измами, която създава автоматизирани цифрови следи, за да заблуждава противниците да мислят, че проникват в мрежите на организацията. Този иновативен подход за киберсигурност позволява на CounterCraft да получава информация за нападателите и целите, като същевременно ги насочва погрешно.

Кампаниите за контраразузнаване отнемат много време за проектиране и сложни за реализиране и поддръжка. Наблюдението им може да бъде трудна, ако не и невъзможна задача. Трудно е да се оцени успехът на такава кампания и да се предостави полезна информация като резултат.

Решението на CounterCraft реализира базирани на заблуда кампании и предлага задълбочен мониторинг и комплексни действия за реакция. Понастоящем платформата за противодействие на кибер измами се използва от правителства, правоприлагащи органи и компании от Fortune 500, доставяйки знания и опит в ИТ сигурността. CounterCraft управлява автоматизирани контра-разузнавателни инструменти за откриване на целенасочени атаки с активен отговор в реално време и нула фалшиви положителни сигнали.

Връзки към киберинституции

Връзки към български, британски и международни органи

- ENISA – Агенция на Европейския съюз за киберсигурност
- ISACA – Международна професионална асоциация, фокусирана върху управлението на ИТ
- ECSO – Координатор на развитието на Европейската екосистема за киберсигурност
- Cybercrime.bg
- CounterCraft
- ESI CEE

Обратна връзка

За въпроси и препоръки

E-mail: acerta@bas.bg

Редакционен съвет

Академична CERT (ACERTA) организация съгласно споразумение, подписано от група академични органи (ИИКТ, ИО-МО, ЕСИ-ЦИЕ, като начало), за засилване на сътрудничеството в изследванията, свързани с киберсигурността

Публикуването на бюлетина се реализира с финансовата подкрепа на Британското посолство в София.

Бюлетинът отразява гледната точка на авторите.

British Embassy Sofia

ИИКТ
Институт по информационни и комуникационни технологии

Институт по отбрана - МО

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE

DIGILIENCE Conference Series
https://digilience.org