CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

*Екип за реагиране при инциденти в компютърната сигурност*

# Мониторинг на актуалните киберновини – към 03.06.2020 г.


## Съдържание

# Microsoft отстранява сривовете в Outlook в юнските актуализации на Office 2020

2 юни 2020 г.

Microsoft пусна актуализации на Microsoft Office, които не са свързани със сигурността, включващи подобрения в производителността и поправки на проблеми, засягащи изданията на Windows Installer (MSI) на продуктите на Office 2016, Office 2013 и Office 2010.

Ъпдейтът KB4484398 адресира периодични сривове в Outlook 2016 и проблемът споделени папки да изчезват от Favorites, когато Outlook стартира в офлайн режим.

Ъпдейтът KB4484392 коригира друг проблем при сривовете, засягащ Excel 2016 и PowerPoint 2016 в някои много специфични сценарии.

Microsoft адресира и грешки, причинени от импортирането на данни от приложения на Microsoft Office, използващи Power BI и използване на SSIS (SQL Server Integration Services) за зареждане на данни от приложения на Office в SQL Server в KB4484394.

Шест от актуализациите на Office, несвързани със сигурността, се отнасят за целите софтуерни пакети Microsoft Office 2016, Microsoft Office 2013 и Microsoft Office 2010, докато други две адресират проблеми, засягащи OneNote 2016 и Outlook 2016.

Актуализациите от юни 2020 г., публикувани от Microsoft, могат да бъдат инсталирани ръчно от Центъра за изтегляне или с помощта на услугата Microsoft Update за автоматична инсталация.

Тези актуализации на Microsoft Office се отнасят само за продукти на Office на базата на Microsoft Installer (.msi) и не се прилагат за издания като Microsoft Office 365 Home.

Списъкът на актуализациите, е достъпен по-долу.

| **Office Product** | **Knowledge Base article** |
|---|---|
| Microsoft Office 2016 | KB4484171 |

| | |
|---|---|
| Microsoft Office 2016 | KB4484335 |
| Microsoft Office 2016 | KB4484392 |
| Microsoft Office 2016 | KB4484394 |
| Microsoft OneNote 2016 | KB4484329 |
| Microsoft Outlook 2016 | KB4484398 |
| Microsoft Office 2013 | KB4484356 |
| Microsoft Office 2010 | KB4484377 |

Някои актуализации може да изискват рестартиране.

Ако инсталацията на вашия Office започне да работи неправилно след актуализиране, можете да деинсталирате проблемната актуализация, като използвате следната процедура:

1. Отидете на Start, въведете View Installed Updates в полето за търсене на Windows и натиснете Enter.
2. В списъка с актуализации намерете и изберете актуализацията и след това изберете Uninstall.

В зависимост от инсталираната от вас актуализация на Office, може да се наложи да приложите и други актуализации, за да бъде проблемът напълно коригиран на вашия компютър (например KB4484356 изисква инсталиране на Microsoft Office 2013 Service Pack 1).

**За повече информация:**

**https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-outlook-crashes-in-june-office-2020-updates/**

# Десет най-добри съвета на ENISA за кибер хигиена по време на пандемията от COVID-19, насочени към малките и средни предприятия

02 юни 2020 г.

По време на пандемията COVID-19 Европейската агенция за киберсигурност публикува десет съвета за кибер хигиена, за да подпомогне малките и средни предприятия (МСП) при защитата на техните виртуални активи от кибератаки.

Кризи като сегашната пандемия имат сериозно влияние върху европейското и международното общество и икономика. Малките и средните предприятия (МСП) трябва да се справят с трудните времена. За съжаление, киберпрестъпниците често виждат такива кризи като възможности. Фишинг и ransomware атаките нарастват.

МСП също са изправени пред нова реалност, в която служителите работят повече от дома. По този начин те стават дори по-зависими от информационните технологии (ИТ) от преди. Безспорно е, че защитата на тези виртуални активи е от изключително значение за почти всяко МСП. Според ENISA, най-добрите десет теми за киберхигиена, които МСП трябва да адресират, евентуално чрез аутсорсинг, когато е необходимо, са представени по-долу:

1. **Управленска заинтересованост.** Важно е ръководството да вижда значението на киберсигурността за организацията и да се информира редовно.

2. **Оценка на риска.** Това отговаря на въпроса: какво трябва да бъде защитено и от какво? Определете и приоритизирайте основните активи и заплахи, пред които е изправена вашата организация.

3. **Политика за киберсигурност**. Създайте необходимите политики за справяне с киберсигурността и назначете някого, например служител по сигурността на информацията (ISO), който отговаря за надзора върху прилагането на тези политики.

4. **Информираност.** Служителите трябва да разбират рисковете и да бъдат информирани как да се държат онлайн. Хората са склонни да забравят подобни неща доста бързо, така че повтарянето от време на време може да бъде ценно.

5. **Актуализации**. Поддържането на сървъри, работни станции, смартфони и др. е ключово за вашата кибер хигиена. Прилагането на актуализации за сигурност е част от този процес. В идеалния случай целият този процес е до определено ниво автоматизиран и актуализациите могат да бъдат тествани в тестова среда.

6. **Архивиране.** Преди да извършите актуализации, жизненоважно е да имате добри резервни копия. Архивирайте най-важните данни често и помислете за цената на загубата на данни. Дръжте резервните копия офлайн, тествайте архивите и се опитайте да имате дублиране на резервните копия.

7. **Управление на достъпа.** Да има правила / политики за управление на достъпа и те да бъдат прилагани. Уверете се, че паролите по подразбиране са променени, че не се споделят и т.н.

8. **Защита на крайните точки.** Помислете за осигуряването на крайните точки, като инсталирате антивирусен софтуер.

9. **Сигурен отдалечен достъп.** Ограничете отдалечения достъп доколкото е възможно и където е абсолютно необходимо, го активирайте, но по сигурен начин. Уверете се, че комуникацията е криптирана правилно.

10. **План за управление на инциденти**. Трябва да има план как да се справим с инцидент, когато се случи. Различни реалистични сценарии могат да бъдат част от този план. Запознайте се с кого можете да се свържете, когато нещата са проблемни, например с националния Екип за реагиране при инциденти в компютърната сигурност.

**За повече информация:**

**https://www.enisa.europa.eu/news/enisa-news/top-ten-cyber-hygiene-tips-for-smes-during-covid-19-pandemic**