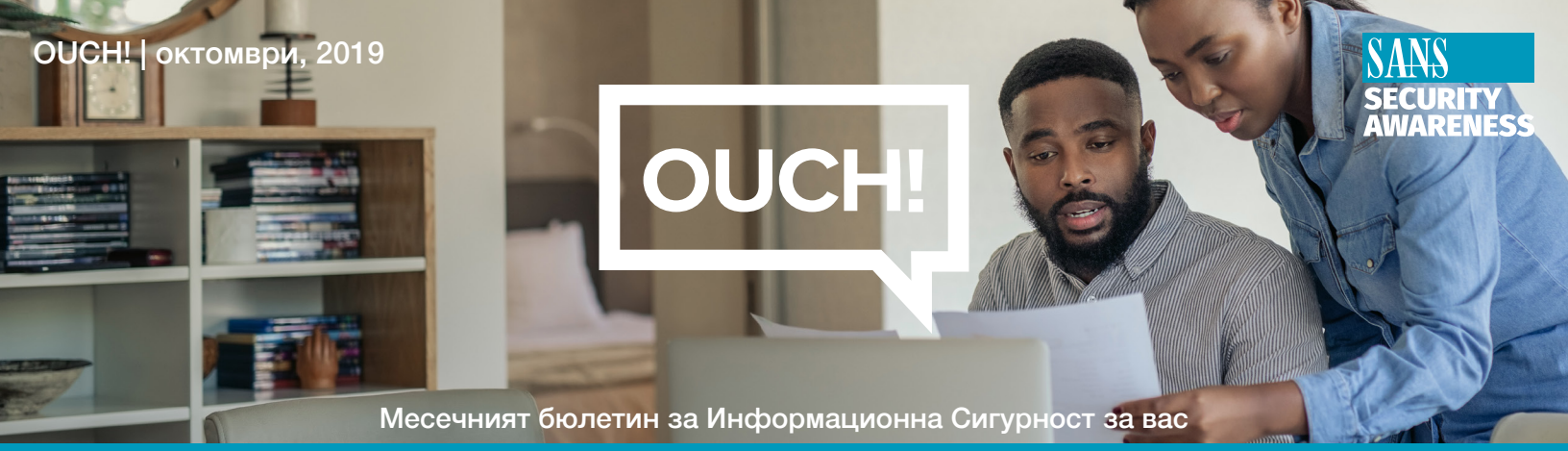

Месечният бюлетин за Информационна Сигурност за вас

Четири прости стъпки към сигурността

Преглед

Работата по сигурността на повечето технологии може да изглежда претоварваща и объркваща. Ето четири прости стъпки, които ще ви помогнат в сигурността независимо от използваната технология.

1. Вие: Първо и най-важно, технологията сама по себе си не може да ви предпази – вие самите сте си най-добрата защита. Хакерите знаят, че най-лесният начин да получат това, което искат, е да атакуват вас самите, вместо компютъра ви или другите ви устройства. Ако искат паролата ви, кредитната ви карта или контрол над компютъра ви, те ще се опитат да ви убедят да им ги предоставите, често с използване на усещане за спешност. Например, могат да ви се обадят, преструвайки се на техническа поддръжка от Майкрософт, твърдейки, че компютърът ви е заразен, докато те всъщност са просто престъпници целящи да получат достъп до компютъра ви. Могат също така да ви пратят имейл, че въображаема пратка за вас не може да бъде доставена, и да поискат да потвърдите адреса си на посочен от тях уебсайт, като всъщност въпросният сайт е предназначен да хакне компютъра ви. Най-добрата защита срещу такива атаки сте самите вие. Използвайки здравия си разум, можете да видите и спрете много атаки.

2. Фрази-пароли: Съвременните мощни компютри направиха класическата 8-символна парола остаряла и уязвима. Когато уебсайт поиска да създадете парола, използвайте силна и уникална фраза. Фразите-пароли са вид парола, която е лесно да се запомни, като например “petar plet plete prez tri pleta”. Колкото по-дълга е фразата, толкова е по-силна. Уникална фраза-парола означава използване на различна такава за всяко устройство или онлайн акаунт. По този начин, ако една от тях е компрометирана, всички останали акаунти и устройства са в безопасност. Не можете да помните всичките тези фрази? Използвайте мениджър за пароли, което е специализирана програма съхраняваща всичките ви пароли в криптиран формат (както и много други полезни неща).

Последно, но не по важност – включете удостоверяването в две стъпки (наричано two-factor или multi-factor authentication). То използва паролата ви, но добавя втора стъпка, като например код изпратен на

телефона ви или приложение, генериращо код. Това е може би най-важната стъпка, която можете да направите, за да защитите онлайн акаунтите си, и е много по-лесно отколкото си мислите.

3. Обновяване: Уверете се, че всяко един от компютърните ви устройства, телефони, програми и приложения работят с най-новата версия на софтуера. Хакерите постоянно търсят нови уязвимости в софтуера, който устройствата ви използват. Когато открият уязвимост, с помощта на специални програми те се възползват от уязвимостта, за да проникнат в устройствата, които ползвате. В същото време компаниите, които са създали софтуера за тези устройства работят усилено по премахването на тези уязвимости и публикуването на обновления. Правейки така, че компютрите и устройствата ви да инсталират тези обновления скоро след публикуването им, правите задачата по хакването им много по-трудна. За да е постоянно обновено всичко, просто активирайте автоматичното обновяване, където е налично. Това правило се отнася за почти всяка технология с мрежова връзка, включително умни телевизори, бебефони, камери, домашни рутери, игрови конзоли и дори автомобили.

4. Архив и възстановяване: Понякога, колкото и да сте внимателни, е възможно да бъдете хакнати. Ако се случи, често единственият начин да възстановите информацията си, е от архив. Уверете се, че правите редовни архивни копия на важната си информация, и проверете, че можете да възстановите данните си от архива. Повечето операционни системи и мобилни устройства поддържат автоматично архивиране на външно устройство или в облачна услуга.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Гост-редактор

SANS сертифицираният инструктор Стивън Ансън консултира екипи по информационна сигурност, както и правителствени организации от различни части на света. Стийв е автор на подготвящата се за печат книга „Applied Incident Response“ и предоставя безплатни ресурси за професионално практикуващите в сферата на информационната сигурност на www.AppliedIncidentResponse.com.

Ресурси

Социален инженеринг:	https://www.sans.org/u/W3G
Персонализирани измами:	https://www.sans.org/u/W3Q
Лесни пароли:	https://www.sans.org/u/W3V
Архивиране:	https://www.sans.org/u/W40