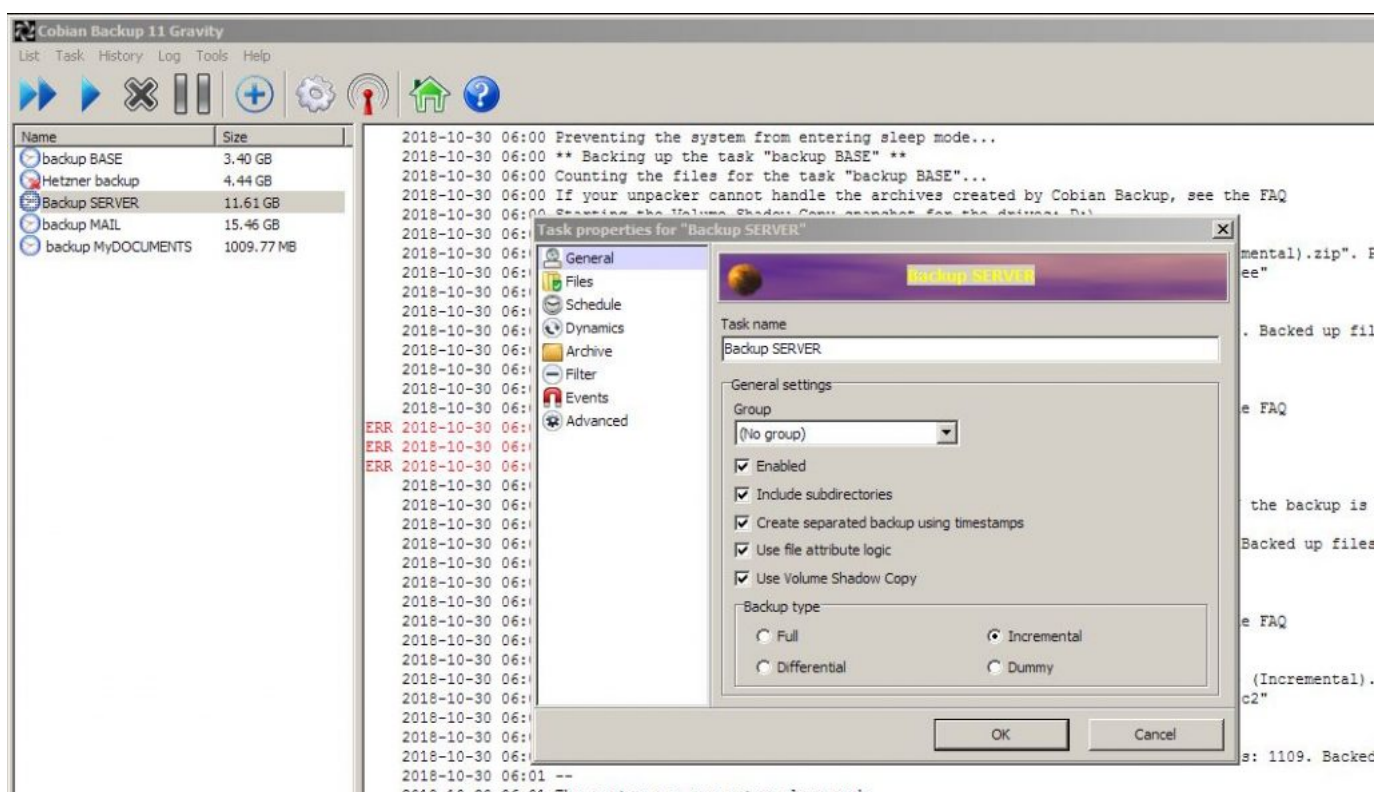


Zaštita od virusa

Virusi su najveća opasnost po vaše podatke, veća čak i od hardverskih havarija. U slučaju da vam se pokvari računar ili disk, skoro uvek se mogu povratiti svi ili bar neki podaci. Ali ako vas “napadne” neki krypto virus, ostaćete bez svih podataka. Zato je veoma bitno da se dobro zaštitite. To nažalost nije tako jednostavno, pa je uvek dobra ideja da angažujete nekog stručnjaka ko će vam pomoći u tome. Ali, ako se pridržavate nekih pravila, bićete mnogo teži plen i smanjićete mogućnost gubitka podataka. Evo koje su najvažnije preporuke koje možete sami da uradite:

Redovno radite bekap. Ova stavka nije slučajno na prvom mestu. U pitanju je jednostavna i brza operacija koju treba raditi **svaki dan**. Dakle, ne nedeljno, mesečno, nego baš svaki dan! Napravite proceduru koju ćete raditi svaki dan ili još bolje napravite automatizovan proces koji će svaki dan posle radnog vremena snimati sve vaše važne podatke na bezbedno mesto. Ako se kasnije nešto i desi, uvek imate podatke od prethodnog dana. Dodatna prednost je što se tako štitite i od hardverskih kvarova i nenamernih grešaka. Na primer, ako nešto važno greškom izbrišete, možete to bez većih problema vratiti.

Postoje specijalizovani programi za bekap podataka koji imaju razne korisne mogućnosti. Možete koristiti besplatni Cobian Backup (<http://www.cobiansoft.com/index.htm>) koji omogućava da podesite sve što želite da čuvate i on će u zadato vreme to da uradi.



Veoma je bitno gde se čuvaju bekap fajlovi. To ne može biti neki od postojećih računara, jer će eventualna havarija ili virus oštetiti sve računare u mreži. Zato se bekap mora čuvati na eksternom računaru, disku ili USB memoriji. Najbolje je recimo zakupiti Google Backup pa će vaši podaci biti na nekom drugom serveru.

App ima ugrađen sistem za bekap koji radi tako što se prilikom izlaska iz programa korisniku nudi snimanje svih menjanih programa. Ovo je korisna opcija koju treba da koristite, ali imajte u vidu da je ovo samo snimak App programa i podataka, tako da se ne čuvaju svi vaši podaci (tekstovi i sl). Takođe je nedostatak to što korisnik jednostavno može da izabere opciju da se ne radi bekap. Zato je preporučljivo da imate nezavisan sistem za bekap svih važnih podataka.

Za backup možete koristiti i opciju Ostalo/Prenos podataka/Wings Cloud backup. Tada se snimljeni podaci prebacuju na naš server, pa su sigurni u slučaju da se desi havarija na vašem računaru.

Instalirajte kvalitetan anti-virus program. Na svakom računaru morate imati uredno ažuriran i podešen program za detekciju virusa (AV program). Noviji Windows sistemi dolaze sa ugrađenim AV programom (Windows 8 i 10) koji je solidna zaštita. Postoji velika ponuda komercijalnih AV programa, mi vam preporučujemo popularni Nod (<https://www.eset.com/us/home/antivirus/>). Izbegavajte da koristite paralelno više AV programa, jer može doći do problema u radu. Svaki AV program mora biti ispravno podešen, inače vam može drastično usporiti rad u App programu.



ESET NOD32
Software

eset
NOD 32
antivirus system

ESET NOD32 Antivirus, commonly known as NOD32, is an antivirus software package made by the Slovak company ESET. ESET NOD32 Antivirus is sold in two editions, Home Edition and Business Edition.
[Wikipedia](#)

Initial release date: 1987
Written in: Assembly language
Original author: ESET

People also search for [View 10+ more](#)

eset INTERNET SECURITY
ESET Internet Security

Avast Antivirus

AVG AVG AntiVirus

Nor by Syrr Norton AntiVirus

KASPERSKY Kaspersky Anti-Virus

Zapamtite da AV program nikako nije 100% zaštita od svih pretnji – on samo smanjuje mogućnost zaraze, ali i dalje morate voditi računa o tome šta radite i pridržavati se opštih preporuka.

Nemojte otvarati mejlove za koje niste 100% sigurni od koga su. Najveći broj virusa se danas dobija preko mejla. Na primer, možete dobiti mejl od nekog poznanika ili poslovnog partnera u kome vas poziva da kliknete na neki interesantan link ili da vidite neku sliku ili video. Kako da prepoznate takav mail pogledajte ovde.

Nemojte raditi pod administratorskim nalogom. Administrator ima prava da radi sve operacije na računaru i ako se virus aktivira može vam uništiti sve podatke. Međutim, ako radite

pod posebnim nalogom koji nema recimo pravo da instalira programe, briše backup i slično, virus neće moći da napravi skoro nikakvu štetu. A za svakodnevni rad je običan nalog sasvim dovoljan.

Šta raditi ako sumnjate da ste zaraženi virusom? Ako ste kliknuli na neki sumnjiv link i sumnjate da ste zarazili svoj računar, nemojte nikako raditi dalje na tom računaru, jer mnogi kriptovirusi uništavaju baš fajlove koje vi redom otvarate. Ugasite odmah računar i potražite stručnu pomoć. Ako radite u mreži, isto uradite sa ostalim računarima.

VAŽNA NAPOMENA: Pobrajane preporuke su samo opšte smernice, nikako nisu konačni spisak svih potrebnih mera zaštite. Savetujemo vam da angažujete profesionalno lice koje će vam podesiti sistem i posavetovati vas kako da organizujete zaštitu vaših podataka.