VARNOSTNE KOPIJE V ČASU POVEČANIH NAPADOV Z IZSILJEVALSKO PROGRAMSKO OPREMO

mag. Simon Abolnar
Šolski center Nova Gorica, Cankarjeva 10, 5000 Nova Gorica
Simon.abolnar@scng.si

Povzetek

V zadnjem času se povečuje število napadov vdiralcev v omrežja in infrastrukturo organizacij. Eden pogostih ciljev vdiralcev je napad z izsiljevalsko programsko opremo. Če vdiralcem napad uspe, je zadnja obramba zaščita varnostnih kopij. V kolikor vdiralcem uspe šifrirati ali zbrisati varnostne kopije, organizacije ostanejo brez vseh podatkov.
Osnova zaščite temelji na ustrezni infrastrukturi varnostnih kopij. Pri tem potrebujemo primarni in sekundarni strežnik za varnostne kopije ter repozitorije za njihovo shranjevanje. Za repozitorije največkrat uporabljamo DAS, NAS in SAN diskovna polja, prostor za shranjevanje v oblaku ter tračne enote. Poleg tega je pomembna ustrezna segmentacija ter zaščita omrežja in ustrezna umestitev infrastrukture varnostnih kopij (strežnikov in repozitorijev).
Za zaščito varnostnih kopij je primerna uporaba kombinacij različnih rešitev. V prispevku je posebna pozornost namenjena posnetkom NAS in SAN diskovnih polj in časovno nespremenljivim Linux repozitorijem.
Poleg tehničnega vidika zaščite varnostnih kopij, je zelo pomemben tudi ekonomski vidik, saj si želimo stroškovne učinkovitosti implementiranih rešitev.

Abstract

BACKUP COPIES AT THE TIME OF INCREASED RANSOMWARE ATTACKS

Recently, the number of attacks by intruders on the networks and infrastructure of organizations has been increasing. One common target of intruders is a ransomware attack. If the invaders attack succeeds, the last defense is backup protection. If intruders manage to encrypt or delete backups, organizations lost all data.

The basis of protection is an appropriate backup infrastructure. We need a primary and secondary backup server and repositories for backing up. For repositories, we mostly use DAS, NAS and SAN disk arrays, cloud storage and tape drives. In addition, proper network segmentation, protection and proper placement of backup infrastructure (servers and repositories) are important.

To protect backups, it is appropriate to use combinations of different solutions. The paper pays special attention to NAS and SAN disk snapshots and Hardened Linux repositories.

In addition to the technical aspect of backup protection, the economic aspect is also very important, as we want the cost-effectiveness of the implemented solutions.

Ključne besede

varnostna kopija, napad z izsiljevalsko programsko opremo, repozitorij, NAS in SAN diskovna polje, tračna enota, prostor v oblaku, časovno nespremenljiv Linux repozitorij

Key words

Backup, Ransomware Attack, Repository, NAS and SAN disk array, Tape drive, Cloud storage, Linux hardened repository

UVOD

Varnostne kopije igrajo zelo pomembno vlogo v okviru IKT znotraj organizacij.

Medtem ko smo bili pred časom predvsem zaskrbljeni glede odpovedi določene strojne opreme ali težav s programsko opremo, se je danes fokus preusmeril na težave, povezane s kibernetsko varnostjo. Napadi v omrežja znotraj organizacij so vedno pogostejši in vse bolj načrtovani. Pogost cilj vdiralcev je napad z izsiljevalsko programsko opremo. Vdiralci izkoristijo kakršnokoli varnostno pomanjkljivost, prevzamejo nadzor nad IKT infrastrukturo ter namestijo izsiljevalsko programsko opremo, s katero šifrirajo vse programske vire znotraj organizacij. Pogosto uspejo šifrirati ali zbrisati tudi repozitorije varnostnih kopij. Vdiralci zahtevajo plačilo relativno visokega zneska za pridobitev kode za dešifriranje podatkov.
Posledice za organizacijo so lahko katastrofalne, saj lahko čez noč ostanejo brez vseh storitev in podatkov. Nekatere od njih se v obupu pogodijo za plačilo visoke odkupnine, vendar tudi plačilo ne daje nikakršne garancije za dejansko dešifriranje podatkov.

Seveda si vsi želimo, da vdore preprečimo, vendar se moramo sprijazniti s tem, da število IKT storitev znotraj organizacij raste in žal obstoja realna možnost, da do vdora pride. Pri vsem tem gre za zelo pomembno vprašanje, kako v tem primeru zaščititi varnostne kopije.

Nadaljnji predmet obdelave bodo infrastruktura varnostnih kopij, segmentacija in zaščita omrežja ter učinkoviti in ekonomični načini zaščite varnostnih kopij.

INFRASTRUKTURA VARNOSTNIH KOPIJ

Že dolgo samo ena varnostna kopija za varno shranjevanje podatkov ne zadostuje. V praksi je potreben najmanj standard 3-2-1:
- najmanj tri kopije podatkov (produkcija, varnostna kopija, kopija varnostne kopije),
- uporaba najmanj dveh različnih medijev za repozitorije varnostnih kopij in
- vsaj ena varnostna kopija na oddaljeni lokaciji ali varnostna kopija brez povezave.

Za varnostne kopije potrebujemo primarni in sekundarni strežnik za varnostne kopije. S primarnim strežnikom poskrbimo za eno ali dve kopije podatkov ter varnostne kopije sekundarnega strežnika, sekundarni strežnik pa služi za varnostne kopije primarnega strežnika ter služi kot nadomestni strežnik, v primeru odpovedi primarnega strežnika.

Dandanes se zelo hitro veča količina podatkov, ki jih moramo varnostno kopirati. Temu primerno moramo poskrbeti za ustrezne repozitorije varnostnih kopij. Poleg tega je zelo pomembna prenosna hitrost omrežja, preko katerega izvajamo varnostne kopije. Zaradi velike količine podatkov so zaželena omrežja s prenosnimi hitrostmi od 10 Gb/s naprej.
Pomembno je tudi, da se repozitoriji nahajajo v drugi stavbi oz. na drugi lokaciji, kot produkcijski računalniki oz. strežniki, saj na ta način zaščitimo kopije v primeru požara, kraje ali drugih nevarnosti.
Programska oprema za varnostne kopije v splošnem podpira razne tipe repozitorijev:
- DAS, NAS, SAN diskovna polja,
- prostor za shranjevanje v oblaku in
- tračne enote.

Tipi repozitorijev se bistveno razlikujejo med seboj tako v kontekstu implementacije varnostnih kopij kot v primeru potencialnega napada z izsiljevalsko programsko opremo, zato je potrebna podrobnejša analiza njihovih lastnosti.

DAS, NAS, SAN DISKOVNA POLJA

Najpogosteje v praksi uporabljamo DAS, NAS ali SAN diskovna polja v lokalnem računalniškem omrežju. V tem primeru lahko izvajamo varnostno kopiranje inkrementalno (glede na potrebe tudi večkrat dnevno) ali v celoti (navadno tedensko ali mesečno). Pri tem lahko koristimo infrastrukturo hitrega lokalnega računalniškega omrežja s prenosnimi hitrostmi nad 10 Gb/s.

Pri vseh omenjenih diskovnih poljih obstaja nevarnost, da bodo vdiralci uspeli šifrirati vse varnostne kopije repozitorijev, v kolikor jim bo uspelo prevzeti nadzor nad strežnikom za varnostne kopije. To predstavlja velik problem v kontekstu dandanašnjih napadov.

Omenjena polja so splošno uporabna in relativno poceni. Danes lahko sestavimo zelo poceni diskovna polja velikih kapacitet. Rešitev je primerna za male, srednje in velike organizacije.

PROSTOR ZA SHRANJEVANJE V OBLAKU

Varnostne kopije v oblaku so zanimiva in pogosto uporabljena rešitev, saj gre za relativno varno rešitev in zelo malo možnosti je, da vdiralci prevzamejo nadzor nad njimi.

V splošnem je zmotno mišljenje, da so podatki v oblaku bolj varni od tistih v našem lokalnem omrežju. Če uspe vdiralcu prevzeti nadzor nad strežnikom za varnostne kopije, lahko posledično tudi šifrira ali izbriše varnostne kopije v oblaku. Zato današnji moderni oblaki omogočajo uporabo zaščite: »zapiši enkrat, preberi večkrat (WORM)« v obdobju določenega obdobja (določenega števila dni). To je vsekakor zelo dobra zaščita pred napadi z izsiljevalsko programsko opremo, saj vdiralcem onemogoča uničenje varnostnih kopij.

Za shranjevanje v oblaku veljajo določene zakonitosti. Navadno je hitrost prenosa podatkov veliko nižja, kot v primeru lokalnega omrežja. Smiselno je redko izvajanje celovitih varnostnih kopij. V praksi strežniki za varnostne kopije prenašajo v oblak dnevne inkrementalne varnostne kopije, ki so po obsegu veliko manjše od celovitih varnostnih kopij. Kljub počasnejši povezavi, pa je tako izvajanje varnostnih kopij hitro.

Prostor za shranjevanje v oblaku je relativno drag. Pri tem se obračunavajo tako stroški samega repozitorija, kot tudi prenosa podatkov ter vzdrževanja rešitve. Organizacije lahko dobijo možnost uporabe oblaka brezplačno ali relativno poceni v povezavi z nakupom drugih oblačnih storitev oziroma v okviru kakšne druge pogodbe.

Eden od pomembnih ponudnikov oblačnih storitev za potrebe varnostnih kopij je Amazon s svojim omrežjem S3 [1].

TRAČNE ENOTE

Tračne enote so ena od rešitev, ki so na prvi pogled najbolj primerne v boju zoper napadom z izsiljevalsko programsko opremo. Vdiralec prav gotovo ne more nič kaseti, ki leži v našem predalu. Pogosto se uporabljajo tudi kasete: »zapiši enkrat, preberi večkrat (WORM)«.

Podrobnejša analiza pokaže, da rešitev ni tako idealna kot se zdi. Varnostna kopija hitro zastara, zato jo je potrebno pogosto obnavljati. Tračno enoto mora nadzorovati strežnik za varnostne kopije. V primeru, da vdiralec prevzame nadzor nad strežnikom, lahko varnostne kopije na kaseti, ki je v tračni enoti, preprosto izbriše (razen v primeru uporabe kasete WORM). V vsakem primeru je potrebno kasete pogosto menjavati, ker varnostne kopije hitro zastarijo. Vse to zahteva veliko administrativnega dela in je bolj primerno za dolgoročne varnostne kopije ali arhiviranje podatkov.

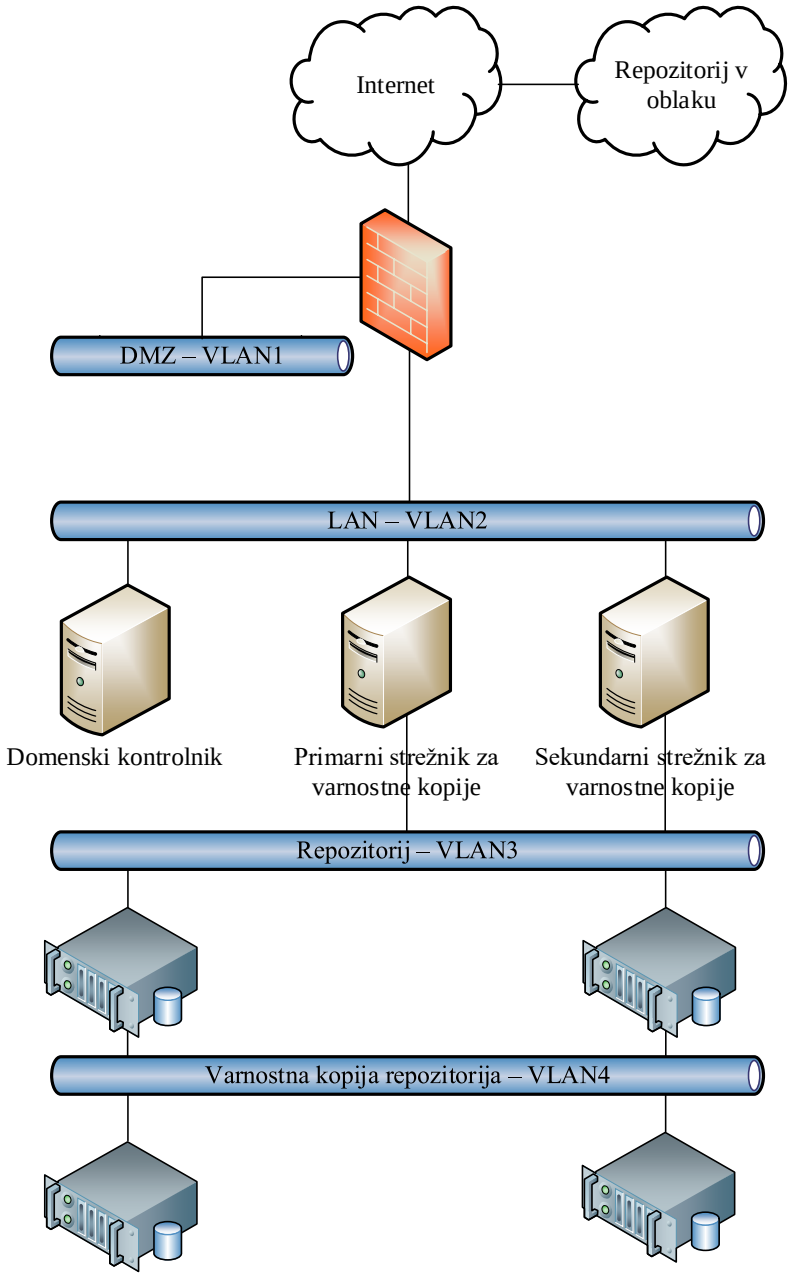
Zmogljivejše tračne enote imajo vgrajen tudi izmenjevalnik kaset. Tudi tu velja podobno pravilo. Nadzor nad izmenjevalnikom lahko pomeni izbris varnostnih kopij, zato je stoodstotno varna le kaseta, ki se ne nahaja v izmenjevalniku ali uporablja način zapisa WORM.

Hitrost zapisovanja in branja podatkov s kaset je omejena in je veliko nižja od 10 Gb omrežja.

Tračne enote in posebej izmenjevalniki niso poceni, vendar so kasete ena najcenejših oblik shranjevanja podatkov. V primeru uporabe kaset WORM, bomo potrebovali bistveno več kaset, kar bo posledično podražilo obravnavane varnostne kopije. V praksi je potrebno zagotoviti, da strežnik za varnostne kopije lahko krmili tračno enoto, oz. izmenjevalnik. Kot je bilo že zapisano, se mora nekdo stalno ukvarjati z omenjeno rešitvijo, kar navadno ni primerno za manjše organizacije.

SEGMENTACIJA IN ZAŠČITA OMREŽJA

Eden od osnovnih mehanizmov zaščite je seveda segmentacija omrežja, ki jo seveda vedno implementiramo znotraj organizacij. Segmentacija je tako ali drugače že prisotna pri zaščiti podatkov in storitev znotraj organizacije.



Slika1: Infrastruktura varnostnih kopij in njihova umestitev v omrežje

Mnogi administratorji omrežja stavijo na zadostno zaščito strežnikov z ustrezno segmentacijo omrežja in nadzorom dostopa do strežnikov. Dandanes so vdiralci zelo iznajdljivi in navadno najdejo način (računalnik, strežnik, itd.), da si kljub implementirani zaščiti zagotovijo dostop do strežnikov v drugem segmentu omrežja. Vseeno moramo narediti vse, da so računalniški viri optimalno zaščiteni.

Pri umestitvi infrastrukture varnostnih kopij v omrežje je pomembno razmisliti o primarni funkciji varnostnih kopij znotraj organizacij. V primeru odpovedi strojne opreme, napake v programski opremi ali napačnega izbrisa datotek in podatkov, želimo čimprej odpraviti težavo in restavrirati stanje s pomočjo ustrezne varnostne kopije. Čas igra tu pomembno vlogo, zato je smiselno imeti strežnike za varnostne kopije znotraj produkcijskega omrežja, vključene v domensko okolje, kljub temu da so na ta način lažja tarča morebitnih vdiralcev. Če je organizacija večja, je smiselno strežnike za varnostne kopije premakniti v poseben segment omrežja, vendar morajo biti še vedno vključeni v domensko okolje. To je smiselno narediti tudi zaradi morebitnega napada notranjih vdiralcev, kar je lahko problem v večjih organizacijah.
Posebno pozornost pri umestitvi v omrežje pa zahtevajo repozitoriji varnostnih kopij in varnostne kopije repozitorijev. Tu se dejansko nahajajo dejanske varnostne kopije, zato morajo biti omenjeni viri še posebno skrbno zaščiteni znotraj računalniškega omrežja.

NAČINI ZAŠČITE VARNOSTNIH KOPIJ

Podjetja na področju IKT se vedno bolj zavedajo razširjenih napadov z izsiljevalsko programsko opremo, zato se je v zadnjih letih pojavilo nekaj načinov zaščite varnostnih kopij. Nekateri so že dolgo v uporabi, drugi pa so novejši. V praksi je najboljše implementirati različne načine zaščite in na ta način povečati stopnjo zaščite.
V nadaljevanju bodo analizirane učinkovite rešitve zaščite varnostnih kopij, ki so na voljo tako v večjih kot tudi v manjših organizacijah.

POSNETKI NAS IN SAN DISKOVNIH POLJ

Možnost izvajanja posnetkov diskovnih polj (Snapshots) je že vrsto let ena od funkcij dražjih diskovnih polj, v zadnjih letih pa imajo to funkcijo implementirano tudi cenejši NAS strežniki. Posnetek diskovnega polja temelji na dejstvu, da se bloki podatkov zaklenejo. Kljub temu, da se podatki spremenijo ali zbrišejo, to ne vpliva na zaklenjene bloke podatkov. Administrator lahko kadarkoli restavrira stanje posnetka diskovnega polja. Edina pomanjkljivost omenjene rešitve je določena dodatna poraba prostora, saj je ob spremembi podatkov določenega bloka potrebno hraniti obe različici podatkov. Prejšnje podatke je potrebno v primeru izbrisa podatkov še vedno hraniti. Ob normalni uporabi je potrebno zagotoviti od 10 % do 20 % dodatnega prostora za hranjenje podatkov na diskovnem polju.

Posnetki diskovnih polj so zelo učinkoviti v primeru napada z izsiljevalsko programsko opremo. Vdiralci navadno šifrirajo vse podatke na diskovnih poljih. V primeru posnetka diskovnega polja, lahko zelo hitro restavriramo prejšnje stanje in na ta način praktično takoj obnovimo podatke brez kakršnekoli uporabe varnostnih kopij.
Pri tem se moramo zavedati, da vdiralec ne sme prevzeti nadzora nad diskovnim poljem. V tem primeru bo lahko brez naše vednosti odstranil vse narejene posnetke varnostnih kopij. Zato je potrebno maksimalno zaščititi možnost upravljanja z diskovnim poljem.

Za zaščito podatkov navadno izvedemo avtomatično ciklično izvajanje posnetkov diskovnih polj. Tako imamo implementiranih stalno nekaj posnetkov vsakih nekaj ur. Ko se izvede nov posnetek, se najstarejši zbriše. Poleg tega je smiselno uporabiti še nekaj posnetkov, ki se izvajajo dnevno.

ČASOVNO NESPREMENLJIVI LINUX REPOZITORIJI

Eno od vodilnih podjetji na področju varnostnih kopij, podjetje Veeam, je v zadnjem letu izdalo 11. različico svoje priljubljene aplikacije za varnostne kopije, »Veeam Backup & Replication« [2]. Omenjena različica prinaša inovativno podporo časovno nespremenljivim Linux repozitorijem (Hardened Linux Repositories).

Implementacija repozitorija je enostavna. Na strežnik namestimo eno od Linux distribucij (npr. Ubuntu). Za potrebe varnostnih kopij rezerviramo diskovno polje in kreiramo ustrezni datotečni sistem, nato repozitorij povežemo z aplikacijo za varnostne kopije. Pri tem je zanimivo, da se poverilnice za dostop do repozitorija (uporabnik ne sme biti član skupine Sudo uporabnikov) uporabijo samo pri povezavi aplikacije in repozitorija in se nikamor ne shranijo. Aplikacija komunicira z agentom, ki je nameščen na strežniku, ki ga uporabljamo za repozitorij. Na ta način zagotovimo, da morebitni vdiralec ne more zlorabiti poverilnic za dostop do strežnika za repozitorij, saj te niso nikjer shranjene in se ne uporabljajo.

V okviru repozitorija lahko kreiramo različne imenike, katerim dodelimo določeno število dni, v okviru katerih se varnostne kopije ne morejo niti spreminjati ali brisati (npr. 7 dni, 14 dni, 21 dni, …). Znotraj imenikov se kreirajo varnostne kopije s konfiguriranim obdobjem zaščite. Tudi če vdiralec prevzame nadzor nad strežnikom za varnostne kopije (Veeam aplikacijo), nikakor ne more zbrisati ali šifrirati varnostne kopije v obdobju dni zaščite podatkov.

V kolikor vdiralec dostopi do strežnika za repozitorij kot Sudo uporabnik, lahko preprosto spremeni datum in čas ter zbriše varnostne kopije. Zaradi varnosti je strežnik smiselno vzdrževati samo preko konzole. V tem primeru je najboljše izključiti vse oddaljene dostope do strežnika, če pa to ni mogoče, je potrebno implementirati večfaktorsko overjanje oddaljenega dostopa (npr. SSH) do strežnika. Na strežniku je potrebno zagotoviti redno usklajevanje fizične ure s pomočjo NTP protokola. Onemogočiti je potrebno tudi oddaljene dostope za nadzor in konfiguracijo strežnika, ki so implementirani s strani proizvajalcev strežnikov (HPE iLO, Dell IDRAC, Intel BMC, itd.).

Pomembno je izpostaviti, da se v tem primeru vsi podatki nahajajo znotraj lokalnega računalniškega omrežja. Na ta način nimamo težav z zakonom o varstvu podatkov, kar je v splošnem lahko problem pri prenosu podatkov v oblak.

Opisana rešitev je relativno poceni, saj poleg aplikacije za varnostne kopije Veeam, strošek predstavlja le strojna oprema strežnikov za varnostne kopije in repozitorije, zato je rešitev zelo uporabna tudi v manjših organizacijah.

ZAKLJUČEK

Varnostne kopije igrajo zelo pomembno vlogo na področju IKT. Težava je, da se udeleženci dokler ni prepozno, tega večkrat ne zavedajo. Naloga informatikov je, da poskušajo celovito in kompetentno informirati vodstva in uporabnike znotraj organizacij. Predvsem vodstva se morajo zavedati pomena varnostnih kopij v modernem svetu IKT. V primeru napada dobijo varnostne kopije neprecenljivo vrednost.

Zelo pomembno je poskrbeti za natančno planiranje infrastrukture varnostnih kopij. Napadi z izsiljevalsko programsko opremo so prinesli povsem drugačne scenarije na področju zaščite

podatkov znotraj organizaciji. Potrebno je preigrati vse možnosti, kjer lahko pride do napada, vdora in izgube podatkov. Vdiralcev ne smemo podcenjevati, saj so časi amaterizma že zdavnaj mimo. Po statistiki pride do napada z izsiljevalsko programsko opremo na svetu vsakih 11 sekund.

Pri zaščiti varnostnih kopij moramo uporabiti čim več različnih možnosti. Pri manjših organizacijah se je smiselno odločiti za cenovno učinkovita DAS, NAS ali SAN diskovna polja, v večjih pa po vseh možnostih, vključno z uporabo tračnih enot in shranjevanje podatkov v oblaku. V vsakem primeru je potrebno aplicirati tudi posnetke NAS oz. SAN diskovnih polj za zaščito. Današnja IKT in rešitve na tem področju nudijo različne možnosti, da se uspešno zoperstavimo napadom vdiralcem in zaščitimo naše podatke.

VIRI IN LITERATURA

[1] Amazon. (2021). Amazon S3. Najdeno 29. junija 2021 na spletnem naslovu https://aws.amazon.com/s3/?sc_channel=PS&sc_campaign=acquisition_RU&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CStorage%7CS3%7CRU%7CEN%7CText&sc_content=s3_e&sc_detail=amazon%20s3&sc_category=Storage&sc_segment=293618441715&sc_matchtype=e&sc_country=RU&s_kwcid=AL!4422!3!293618441715!e!!g!!amazon%20s3&ef_id=EAIaIQobChMI19fJ5IP75AIVQeWaCh0lyAGdEAAYASAAEgIHnPD_BwE:G:s

[2] Veeam. (2021). Veeam Backup & Replication. Najdeno 29. junija 2021 na spletnem naslovu https://www.veeam.com/vm-backup-recovery-replication-software.html?ad=menu-products

==========