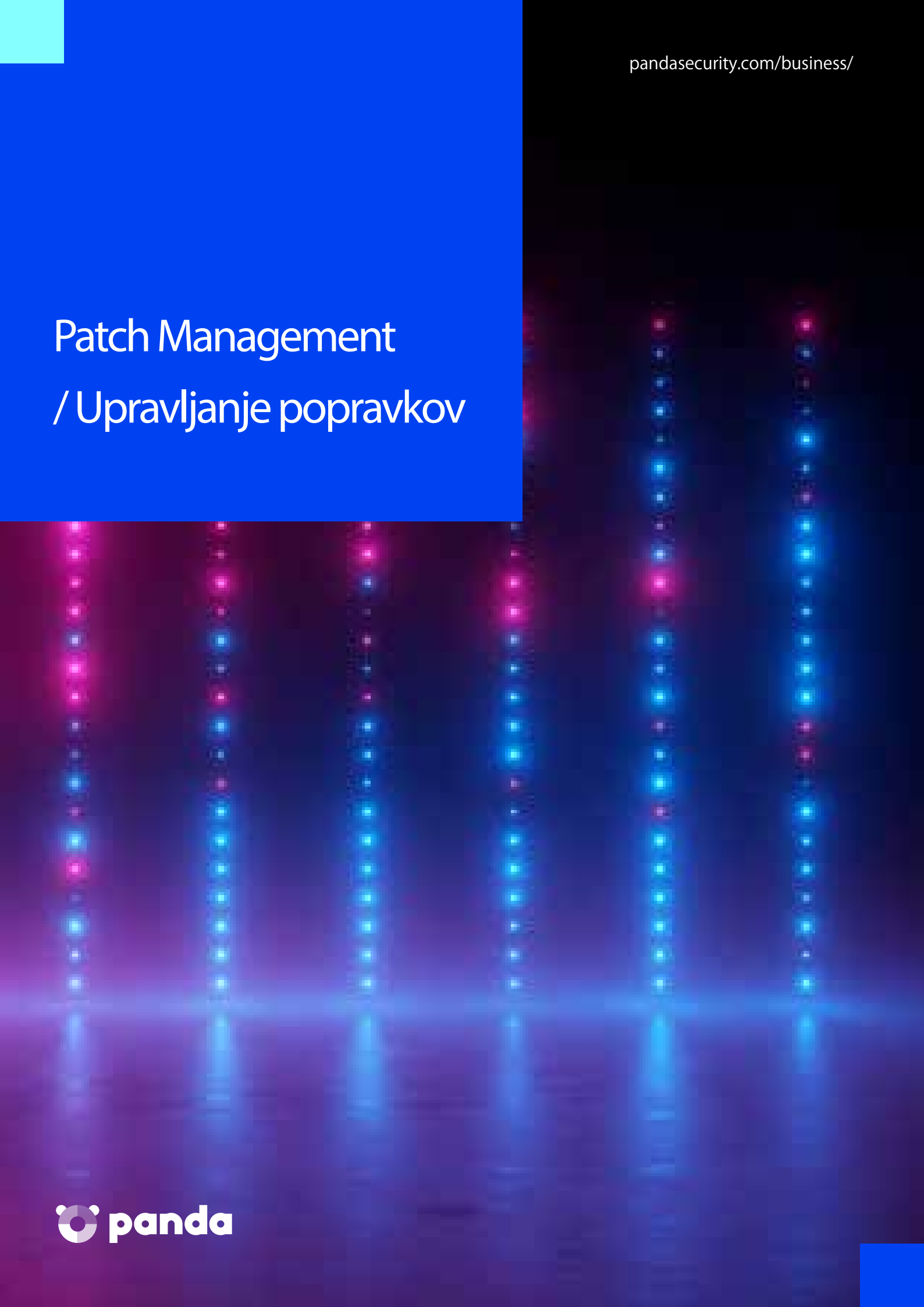
pandasecurity.com/business/

Patch Management / Upravljanje popravkov



panda

Kazalo:

| POMEMBNOST PATCH MANAGEMENTA V ORGANIZACIJI

Popravki programske opreme znajo biti neprijetni za IT upravljalce. Razporejanje popravkov po prioriteti je zamudno opravilo, ne samo za upravljalce, tudi za uporabnike. Računalniki in strežniki morajo biti pogosto ponovno zagnani, kar vodi v prekinitve dela. Zaradi tega so posodobitve pogosto odložene, priporočeni popravki pa se ne upoštevajo. Vendar pa imajo ta, na videz nedolžna, dejanja lahko resne posledice za organizacije.

Prav tako imajo lahko IT upravljalci resne težave pri zagotavljanju, da imajo vsi sistemi znotraj njihovega omrežja nameščene vse potrebne popravke. Programski popravki in posodobitve so ključnega pomena pri zagotavljanju stabilne kibernetske varnosti organizacije, saj onemogočajo izpostavljenost programske opreme in sistema varnostnim grožnjam.

panda

| RANLJIVOSTI V ŠTEVILKAH

V letu 2019 so poročali o 12 174 šibkih točkah glede varnosti. Glede na to dejstvo, ni presenetljivo, da organizacije z omejenimi sredstvi težko vzdržujejo in varujejo vso svojo infrastrukturo.

Patch management je opravilo, ki zahteva veliko časa in sredstev, zato je pogosto zahtevno imeti pregled nad premoženjem in programi, hkrati pa dajati prednost popravkom in imeti možnost hitro »zakrpati« kritične programe in sisteme. Podjetja morajo biti sposobna upravljati popravke kar se da učinkovito, saj bi sicer lahko imeli negativen vpliv na njihovo produktivnost in kibernetsko varnost.

24,1 % (opomba, vir) vseh ranljivosti pripada petih podjetjem: Software in the Public Interest (SPI), SUSE, Oracle, IBM in Microsoft.

Najbolj razširjeni programi drugih proizvajalcev pa so glavna tarča hekerjev. Po navedbah indeksa skupnih ranljivosti in izpostavljenosti (= Common Vulnerabilities and Exposure index, CVE (opomba, vir)), imajo aplikacije, kot so Java, Adobe, Google Chrome, Mozilla Firefox, OpenOffice, ipd., največje število ranljivosti. Torej, le preprosto popravljanje operacijskih sistemov ni dovolj.
Še en dejavnik, ki ga je treba upoštevati, je povečanje števila napadalcev z znanjem, da hitreje odkrijejo ranljivosti. Ko jih enkrat najdejo, nameščajo programe, ki avtomatsko izkoriščajo te nove ranljivosti, ki so široko razširjene, včasih celo virusne. Rezultat kombinacije groženj, ranljivosti in posledic pa predstavlja precejšnje tveganje za podjetja. Čeprav se zdi presenetljivo, neodkrite ranljivosti niso največja nevarnost.

Viri:
1. Cybersecurity alert – TechRepublic

| POZNANE RANLJIVOSTI = VISOKO TVEGANE RANLJIVOSTI

Izkoriščanje ranljivosti je še vedno najbolj pogost vzroki za kršenje varnosti. Zloglasnih primerov kršenja, kot so WannaCry, Petya in BlueKeep (o teh sem že prevajala, mogoče se lahko doda povezava, samo ideja :), se veliko ljudi še zmeraj spomni, saj so povzročili pravo opustošenje po vsem svetu. Le malo število napadov se zgodi kot rezultat neznanih ranljivosti (zero-day attacks = napadi brez dneva?), večinoma so napadene že znane ranljivosti.

Glede na raziskave podjetja Gartner (opomba, vir) bo 99 % vseh izkoriščenih ranljivosti, ki se bodo zgodile do konca leta 2020 že poznanih varnostnim profesionalcem in IT upravljalcem. V nasprotju pa se je zero-day napadov na neznane ranljivosti zgodilo le v 0,4 % v zadnjem desetletju.

Pomembno si je zapomniti, da imajo hekerji dostop za izvajanje napadov, s katerimi ne odlašajo, saj vedo, da večina podjetij ne popravlja svojih sistemov. Pravzaprav 80 % uspešnih napadov izkorišča ranljivosti, za katere so popravki znani, a niso bili uporabljeni.

Glede na vsa ta dejstva je jasno, da si morajo podjetja prizadevati za nadzor in blaženje znanih ranljivosti, ki se znova in znova izkoriščajo – znane ranljivosti so večje in bolj realno tveganje kot druge vrste groženj. Čas med razkritjem ranljivosti in njenim izkoriščenjem se je v zadnjem času občutno skrajšalo, kar prisili podjetja, da delajo noč in dan za namestitev vseh popravkov. Tako lahko preprečijo kibernetskim napadalcem, da ogrozijo njihov sistem z različnimi napadi.

57 % žrtev kibernetskih napadov pravi, da bi nameščanje popravkov pravočasno preprečilo napad.
34 % pravi, da so vedeli za ranljivost pred napadom.

Viri:
3. Focus on the Biggest Security Threats, Not the most Publicized – Gartner
4. Cost and consequences of gaps in vulnerability response – Ponemon

| PATCH MANAGEMENT

a) Kaj management popravkov vključuje?

Management popravkov je proces, ki podjetjem (in njihovim IT oddelkom) omogoča prenos in namestitev popravkov, ki posodobijo, optimizirajo in zaščitijo programsko opremo, računalnike, serverje in sisteme. Namen je, da zagotovijo nemoteno delovanje teh naprav ali ublažitev ranljivosti. Čeprav se morda zdi enostavno opravilo, ima večina podjetij težavo prepoznati, katere so kritične posodobitve, ki bi jih morali namestiti prve. Ravno zato je za upravljalce ključno razvrščanje po prioritetah. Pravzaprav, glede na raziskavo iz Ponemon-a (?), je povprečen čas, ki ga podjetja potrebujejo za popravke programov in sistemov, 102 dni (opomba, vir). Vendar pa za zaznavo kibernetskega napada, ko je popravek za ublažitev varnosti že izšel, v povprečju potrebujejo 43 dni (opomba, vir). Kar pomeni, da je v povprečju 59 dni praznina, čeprav tveganje že obstaja. (Men je čuden stavek, ampak ne znam drugače obrnit)

Viri::
5. State of Endpoint security risk 2018 – Ponemon
6. Cost and consequences of gaps in vulnerability response – Ponemon

b) Katere vrste popravkov obstajajo?

Obstaja več različnih vrst popravkov in vsak ima drugačen namen: popraviti napako ali posebne ranljivosti. To so nekateri primeri: hitri popravki, servisni popravki, različice za vzdrževanje, Monkey patch).

V tem vodiču se bomo osredotočili na dve vrsti popravkov, ki se nam zdita najpomembnejši. Njihov cilj je odpraviti kritične varnostne ranljivosti, ki jih napadalci pogosto izkoriščajo, zato so najpomembnejši za podjetja in strokovnjake za varnost.

- Varnostni popravki – vplivajo na delovanje sistema in programske opreme drugih proizvajalcev: Varnostni popravek je sprememba v programu ali aplikaciji, ki odpravi napako ali pomanjkljivost, ki povzroča ranljivosti. Uporaba takih popravkov preprečuje, da bi bile ranljivosti izkoriščene ali pa izničijo oz. ublažijo možnost groženj za izkoriščanje ranljivosti. Management popravkov je del obvladovanja/upravljanja ranljivosti: ciklična praksa odkrivanja, razvrščanja, sanacije in ublažitev ranljivosti (varnostna tveganja).
- Podporni paket (Service Pack) ali paket posebnosti (Feature Pack): Te popravki so pomembni, saj predstavljajo zbirko za posodobitve, popravke ali izboljšave funkcij za dele programske opreme. Težijo k reševanju čakajočih težav in po navadi vključujejo vse popravke, hitre popravke, vzdrževanja in varnostne popravke, ki so izdani pred podpornim paketom.

c) Čemu služijo popravki?

Popravki so namenjeni odpravljanju ranljivosti ali varnostnih vrzeli, ki so ugotovljene po prijavi v program ali ko se je del programske opreme zagnal.

Nenadgrajena programska oprema lahko izpostavi izkoriščevanju vse končne točke, to ponuja hekerjem odlično priložnost, da uspešno sprožijo napade. Programski popravki so kritičen del delovanja za upravljalce in strokovnjake za varnost.

V tehnološkem oz. programskem sektorju se pogosto zgodi, da po tem, ko je bil program zagnan, potrebuje popravke ali celo spremembe. Zaradi tega je dobro razviti postopek, ki je podoben življenjskemu ciklu programske opreme, kjer so določene različne faze, ki omogočajo analizo, oceno in redno uporabo popravkov za reševanje morebitnih težav.

| ŽIVLJENJSKI CIKEL PATCH MANAGEMENTA

Management popravkov je lahko najbolj efektivno orodje za zaščito podjetja pred ranljivostmi in najcenejše za vzdrževanje, če je učinkovito izvajan. V tem delu vam bomo razložili, kako ustvariti rutinski postopek upravljanja popravkov, z namenom, da bi ga vključili med svoje standardne postopke v podjetju. Ta postopek je sestavljen iz šestih delov (opomba, vir):

1Opredelitev sredstev in osnovne programske opreme:

Prepoznavanje sredstev in katera programska oprema ter popravki so nameščeni na njih je zapletena naloga, vendar izboljša tako varnost kot operativnost. Če imate to osnovo, vam omogoča spreminjanje sistema brez tveganj in omogoča vrnitev v prejšnje znano uporabljeno stanje (known functional state), v kolikor se pojavijo težave med nameščanjem posodobitev ali popravkov.

Razpoložljivost:

Trenutni seznam popravkov mora biti pregledan glede na popis sredstev in programske opreme, z prepoznavanjem, kater popravek vpliva na katero sredstvo.

Uporabnost:

Objavljeni popravki niso vedno veljavni za vse naprave. To pomeni, da je pomembno preveriti, ali je določena posodobitev primerna za vašo napravo.

Pridobitev:

Pridobitev datoteke za posodobitev iz uradnega vira, kot tudi preverjanje, ali je popravek zakonit, ni vedno enostavno

Preverjanje:

Namen preverjanja je zagotoviti, da posodobitev ne bo imela negativnega vpliva na postopek. Za preverjanje popravkov in posodobitev morate uporabiti testna sredstva in jih uporabiti po fazah uvajanja. Preverjanje je namenjeno preverjanju posledic, ki bi jih posodobitve lahko imele, kar bi lahko vplivalo tudi na spremembe nastavitev, pravilnika požarnega zidu, itd.

Uvajanje:

V postopku preverjanja morate ustvariti uvajalni paket, ki vsebuje datoteke za posodobitve in namestitev ter seznam sredstev, kjer je potrebno izvesti uvedbo/uvajanje.

Vir::
7. Patch management in control systems – INCIBE-CERT

| NE PUSTITE ZNANIM RANLJIVOSTIM V SVOJO IT INFRASTRUKTURO Z PANDA PATCH MANAGEMENTOM

Panda Patch Management je rešitev, ki poenostavi kompliciran cikel managementa popravkov za operacijske sisteme in programsko opremo drugih proizvajalcev. Rezultat je, da je zmanjšana površina, ki bi lahko bila napadena, in okrepljena zmožnost preprečevanja in omejevanja incidentov, ki jih povzročijo sistemske ranljivosti.

Rešitev je vključena v Panda Security končne točke varnostnih rešitev, kar pomeni, da ne potrebuje nobenih novih predstavnikov/zastopnikov ali upravljalnih konzol. Omogoča centralizirano vidnost v realnem času v stanje ranljivosti, popravkov, čakajočih posodobitev in nepodprte ali EoL programske opreme v računalnikih in strežnikih, tako znotraj kot zunaj omrežij podjetja. Orodja za upravljanje vam omogočajo avtomatizirati odkrivanje, načrtovanje, namestitev in spremljanje kritičnih popravkov in posodobitev, ki jih vaša organizacija potrebuje. Vse v realnem času in preprostem, intuitivnem/nagonskem ? času.

Med glavne prednosti in značilnosti, ki jih Panda Patch Management ponuja spadajo:

- Zmožnost revizije, spremljanja in določanja prednosti za posodbitve za operacijske sisteme in programe. Omogoča vam prikaz stanja popravkov in posodobitev v čakanju za sistem in stotine aplikacij in programov drugih proizvajalcev. Omogoča vam celo, da popravke »zavrtite« nazaj (v predhodno različico).
- S sistematičnim zmanjševanjem preprečuje površino za napad, ki jo povzročajo ranljivosti. Upravljanje popravkov in posodobitev vam omogoča, da prehitite izkoriščanje ranljivosti.
- Omejuje in blaži napade, ki izkoriščajo ranljivosti, saj takoj namesti kritične posodobitve iz konzole v oblaku. Konzola povezuje zaznave z ranljivostmi in jim tako zmanjša odziv, zadrževanje in čas sanacije – zaradi namestitve posodobitev iz konzole kot je potrebno. To pa omogoča izolacijo prizadetih/okuženih računalnikov iz omrežja, ki vsebujejo tako dejanske kot možne napade.
- Zmanjšani obratovalni stroški, saj ne zahteva nobenih zastopnikov ali posodobitev na končnih točkah – poenostavljen management brez preobremenitve računalnikov ali strežnikov. Zmanjšuje napor oddaljenih posodobitev iz oblaka. Takojšnja, samodejna vidljivost ranljivosti, posodobitev in EoL programov/aplikacij.

Patch management je proces, ki mora biti redno opravljen in čim bolj celovit, da je učinkovit. To ne pomeni, da se vse sisteme obravnava enako; vsako podjetje mora dati prednost svojim sredstvom in zagotoviti, da so najprej zaščiteni najbolj kritični deli.

Kljub temu je pomembno zagotoviti, da so popravki nameščeni na vseh napravah in ne le tistih z največjo vrednostjo in pomembnostjo za poslovanje. Poleg tega obliži ne zahtevajo le truda od sistemskih administratorjev, temveč zahtevajo tudi podporo podjetja, da se dogovori o konkretnem vzdrževanju.

PREPREČEVANJE NAPADOV

Prilagodljiva varnostna arhitektura

Predvidevaj, pričakuj

Odkrijte ranljivosti, čakajoče popravke in posodobitve ter EoL programe.

Prepreči

Samodejno načrtovanje popravkov. Zamenjava EoL programov.

Zaznaj in obvladuj

Patching all vulnerable endpoiZadrževanje napadov s popravki v realnem času.

Reagiraj

Zapis/popravek vseh ranljivih končnih točk.

Ugotovite, kako vam lahko Panda Patch Mnagement pomaga poenostaviti upravljanje ranljivosti z upravljanjem posodobitev in varnostnih popravkov.

Želim demonstracijo / preizkus

Kontakt

Anni d.o.o.
Motnica 7a
1236 Trzin

panda.anni.si

panda