Panda Patch Management

Eliminer risiko og kompleksitet, oppdag enkelt sårbarheter i systemer og tredjeparts applikasjoner

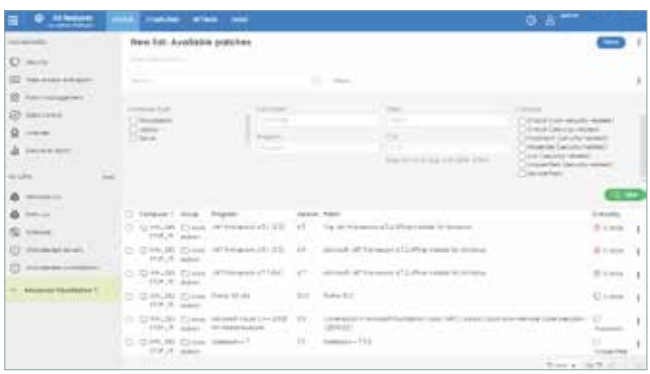
I dag er 99,96% av aktive sikkerhetsproblemer i bedriftens endepunkter relatert til manglende oppdateringer, men dersom de er installert, vil det i stor grad forhindre risikoen. I tillegg skyldes 86% av sikkerhetsproblemene upatchede tredjepartsprogrammer som Java, Adobe, Mozilla, Firefox, Chrome, Flash og Office, osv[1].

Dersom denne trenden fortsetter vil det innen 2020 i 99% av tilfellene som leder til sikkerhetshendelser, skyldes kjente sikkerhetshull som lett kunne vært unngått ved å bli patchet før angrepet[2].

LA OSS FORANDRE DENNE TRENDEN MED PANDA PATCH MANAGEMENT

Panda Patch Management er en brukervennlig løsning for å håndtere sårbarheter for operativsystemer og applikasjoner på Windows-arbeidsstasjoner og servere. Det eliminerer risiko samtidig som du styrker forebygging, beskyttelse og innskrenker angrepsoverflaten i ditt IT-miljø.

Løsningen krever ikke endring for endpoint-agenter eller administrasjonskonsoll, og er fullt integrert i alle Panda Security-endepunktsløsninger. I tillegg gir det sentralisert oversikt i sanntid til sikkerhetsstatus for programvaresårbarheter, manglende patcher, oppdateringer og utdatert (EoL[3]) programvare, innenfor og utenfor bedriftsnettverket, samt brukervennlige og sanntidsverktøy for hele syklusen for patching: fra oppdagelse, planlegging, til installasjon og overvåking.



SÅRBARHETER: EN LATENT RISIKO

Upatchede **operativsystemer og tredjeparts programvare** er den perfekte yngleplass for angrep og infeksjoner som utnytter kjente sårbarheter for uinstallerte patcher som har vært tilgjengelige noen uker, eller til og med måneder før innbruddet.

Den massive delingen av informasjon rundt sårbarheter som deles av Shadow Brokers eller WikiLeaks, med detaljerte instruksjoner om hvordan du kompromitterer både systemer og applikasjoner, gjør det mulig for et voksende antall cyberkriminelle å foreta angrep.

Digital transformasjon gjør det stadig tyngre å redusere angrepsoverflaten, på grunn av det økende antall brukere, enheter, systemer og tredjepartsapplikasjoner som krever tilsyn.

Fem frustrererende operasjonelle problemer med programmer for sårbarhetsstyring (VM):

- **Avsløringsfasen for sårbarheter er for lang**. I tilfeller av sikkerhetshendelser, må responstiden være umiddelbar.
- **Virksomheter er desentraliserte**, ansatte kobler seg ikke konsekvent til jobbnettverket. Derfor vil **interne VM**-verktøy ikke være tilstrekkelige til i slike scenarier.
- De fleste VM-verktøy krever **enda en dedikert agent** på endepunkter som allerede er overbelastet nok som det er.
- VM-verktøy fra Microsoft tillater ikke virksomheter å patche **tredjeparts applikasjoner** på en effektiv, sentralisert og samkjørt måte.
- Andre sikkerhetsløsninger, som inneholder oppdateringsadministrasjon, **korrelerer ikke mellom deteksjon og sårbare enheter** for å sikre rask respons og utbedring.

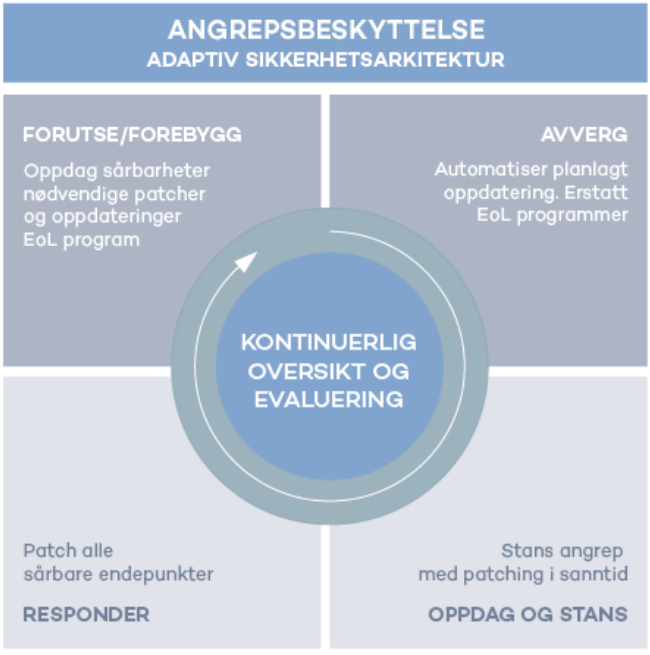
[1] Gartner, Focus on the Biggest Security Threats, Not the most Publicized. Publisert: 2. november 2017. Nulldagstrusler utgjør bare 0,4%, for resten av sårbarheter, 99,96%, er det snakk om manglende oppdateringer. National Vulnerability Database. 86% av sikkerhetsproblemene finnes i tredjepartsprogrammer.
[2] Gartner: How to Respond to the 2018 Threat Landscape. Greg Young. Publisert: 28 november 2017
[3] EoL (End-of-Life): Et produkt som er på eller nesten passert slutten av livstidssyklus (fra leverandørens synspunkt), som dermed kanskje ikke lenger vil motta sikkerhetsoppdateringer.

Panda Patch Management

FORDELER

Panda Patch Management muliggjør, innenfor **en enkelt brukervennlig løsning:**

- **Revisjon, overvåkning og prioritering over operativ-systemer og programoppdateringer**. Visningen med alt på en flate gir en sentralisert minuttvis oppdatert og samlet oversikt i sikkerhetsstatusen til organisasjonen, med hensyn til sikkerhetsproblemer, oppdateringer, ventende oppdateringer av systemer og hundrevis av applikasjoner.
- **Stopp hendelser, reduser systematisk angrepsoverflaten som skyldes sårbarheter i programvare.** Håndtering av patching og oppdateringer via brukervennlig administrasjon i sanntid, som gjør det enkelt for organisasjoner å komme i forkant av angrep.
- **Synliggjør og avgrens årsaker for angrep pga sårbarhet** med kvalifiserte oppdateringer. Adaptive Defense 360-konsollet, i forbindelse med Patch Management, gjør organisasjoner i stand til å oppdage trusler og exploits med å avdekke sårbarheter. Miniml responstid, isolerer sårbarheter og patche umiddelbart med noen få klikk rett i webkonsollen. I tillegg kan berørte maskiner isoleres fra resten av nettverket, ved potensiell lekkasje eller direkteangrep.
- **Reduser driftskostnadene.**
  - **Panda Patch Management krever ikke redistribusjon eller oppdatering for allerede installerte agenter**, noe som forenkler administrasjon og overbelastning for arbeidsstasjoner eller servere.
  - **Minimerer jobben med patching siden disse betjenes eksternt** fra det skybaserte verktøyet. I tillegg er installasjonene optimaliserte for å minimere feil.
  - **Gir uten tilsyn, total oversikt over alle potensielle sårbarheter**, samt nødvendige patcher og EoL[3]-programmer umiddelbart etter aktivering.
- **Vær i tråd med ansvarlighetsprinsippet** som gjelder i flere forskrifter (GDPR, HIPAA og PCI). Sørger for at din virksomhet har tatt de nødvendige tekniske og organisatoriske tiltak for å sikre forsvarlig beskyttelse av sensitive data under deres ansvar.



Panda Patch Management forsterker de preventive, detekterings- og respons-funksjonene til Panda Securitys sikkerhetsløsninger ved å muliggjøre en robust implementering av Adaptive Security Architecture[4]

FUNKSJONER

Panda Patch Management inneholder alle nødvendige verktøy for å sentralt administrere, via skykonsoll, sikkerhet og oppdateringer av operativsystem, samt tredjeparts applikasjoner:

Avdekning:

Ett skjermbilde med sanntidsinformasjon for alle sårbare datamaskiner, ventende patcher og usupportert (EOL[3]) -programvare, med deres status for utbedring.

- Detaljert informasjon om patcher og de neste oppdateringer, detaljer om den relevante sikkerhetsppslag, samt maskin- og gruppeinformasjon med mer. Anbefalte tiltak:
  - Filtrer og se oppdateringer sortert etter alvorlighetsgrad, enheter, grupper, programmer, patch, CVE ID og status.
  - Mulighet for direktehandlinger på enheter: Start, installer med en gang eller legg til senere.
- Automatisk skanning etter oppdateringer, i sanntid eller med intervaller (3, 6, 12 eller 24 timer).
- Varsler om sårbarheter og relevante botemidler. Mulighet til å starte installasjoner umiddelbart eller senere via skykonsoll, man kan isolere maskiner dersom det viser seg nødvendig.

Patchings-, oppdaterings- og installasjonsplanlegging:

- Konfigurerbar etter nivå av alvorlighetsgrad.
- Kan utføres på bestemte endepunkter eller grupper.
- Umiddelbar eller planlagt engangskjøring eller gjentatt eksekvering basert på jevne intervaller (angitt med dato/klokkeslett).
- Mulighet for å kontrollere omstart av maskiner og enheter, samt angitte unntak.

Monitorering av endepunkt og oppdateringsstatus, via:

- Dashboard og handlingslister.
- Kritisk nivå og detaljerte rapporter.
- Lister over oppdaterte maskiner, maskiner med ventende oppdateringer og maskiner med feil.

Administrasjonshistorikk basert på grupper og roller med forskjellige tilgangsnivåer:

- Rollebasert oversikt til sårbare maskiner, patcher, oppdateringer og servicepakker.

Kompatibel med følgende løsninger innenfor Aether Platform:

Panda Endpoint Protection | Panda Endpoint Protection Plus
Panda Adaptive Defense | Panda Adaptive Defense 360

Støttede operativsystemer: Fra Windows XP SP3+. Windows Server 2003 (32/64 bits og R2) SP2+

Støttede tredjepartsprogrammer:
https://www.pandasecurity.com/business/PatchManagementApp

Sertifiseringer og utmerkelser:

Panda Security deltar regelmessig i og mottar priser for beskyttelse og prestasjoner fra Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs.

Panda Adaptive Defense oppnådde EAL2 + sertifisering i evalueringen for Common Criteria-standarden.

"Gartner utnevnte Panda Security som visjonær i Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) i 2018"
https://www.pandasecurity.com/gartner-magic-quadrant/

[4] Gartner: "Design av en adaptiv sikkerhetsarkitektur for beskyttelse mot avanserte angrep", Neil MacDonald, Peter Firstbrook