TeamViewer
Remote Management

WHITEPAPER

Mis nooit meer een patch:

Verlaag beveiligingsrisico's en bescherm uw IT-infrastructuur met geautomatiseerd patchbeheer

Inhoudsopgave

Inleiding:
Wat is een patchbeheeroplossing?

Regelmatig onderhoud en tijdige updates voor alle computers en apparaten zijn vereist om uw IT-infrastructuur veilig en stabiel te houden. Als u uw computers en apparaten niet bijwerkt, kan dit leiden tot aanzienlijke beveiligingsproblemen door verouderde software.

IT-organisaties worden geconfronteerd met nieuwe uitdagingen om ervoor te zorgen dat apparaten altijd up-to-date en 'gepatcht' zijn, vanwege het groeiende aantal bedrijfsapparaten, toepassingen en cyberkwetsbaarheden.

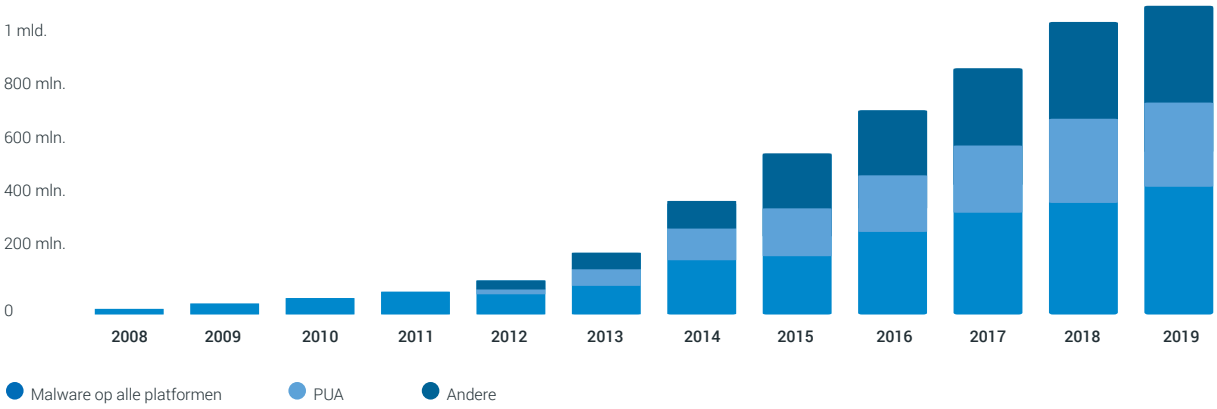
In de IT-wereld is een 'patch' een lijst met specifiek ontworpen wijzigingen die zijn aangebracht in een computerprogramma om het bij te werken, te optimaliseren of te herstellen. Patches kunnen worden gebruikt voor het herstellen van kwetsbaarheden in software en andere bugs, en worden beschikbaar gesteld voor gebruikers door middel van software-updates. Het controleren van de beschikbaarheid van patches en installeren van ontbrekende patches vereist een geautomatiseerde patchbeheeroplossing.

Met een patchbeheeroplossing kunt u verouderde, kwetsbare software detecteren en patchen.

Patching is daarom een essentieel onderdeel van IT-beveiliging. Als u geen patches aanbrengt, worden zwakke plekken in de beveiliging nooit hersteld, waardoor u het gemakkelijk maakt voor hackers en cybercriminelen om bedrijfsgegevens te stelen. Volgens een onderzoek van NIST is 90% van de geslaagde aanvallen op bedrijven te wijten aan bekende kwetsbaarheden en hadden ze voorkomen kunnen worden door correcte, tijdige patching.[1]

Het belang van patchbeheer voor bedrijven

Cyberaanvallen met malware kunnen aanzienlijke schade aanrichten bij bedrijven. Gegevensverlies, reputatieschade of productieonderbrekingen kunnen organisaties miljoenen kosten. Het aantal malwarevarianten neemt bijna dagelijks toe. En dat betekent dat uw IT-infrastructuur efficiënt beveiligingsbeheer vereist.

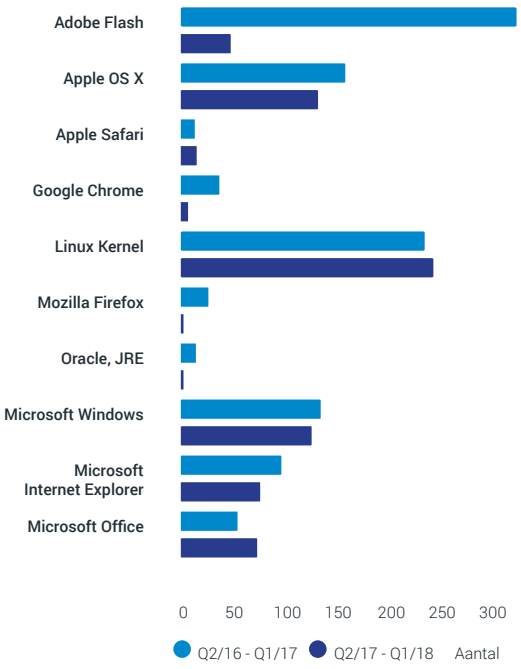


Afbeelding 1: Totale aantal bekende malwarevarianten *PUA (mogelijk ongewenste toepassing)[2]

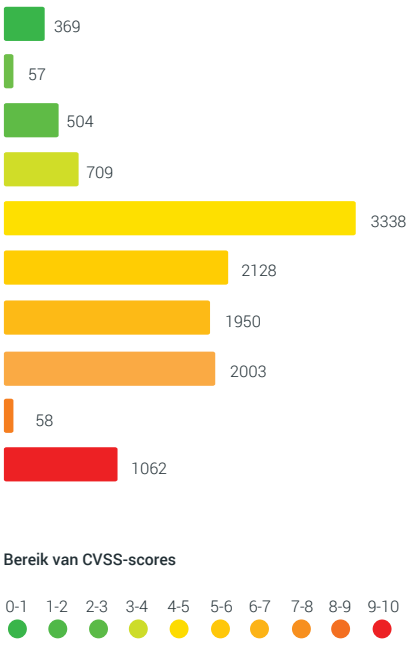
Cyberaanvallen, zoals de ransomewareaanval WannaCry uit 2017, toonden opnieuw aan hoe belangrijk het is om uw hardware en software te beschermen tegen aanvallen. De meeste systemen en toepassingen van grote bedrijven zijn toegankelijk via internet, wat het eenvoudiger maakt voor criminelen om binnen te komen. Antivirussoftware op zichzelf is niet voldoende om IT-infrastructuren volledig te beschermen. Door de grotere complexiteit van software worden er meer fouten gemaakt in de ontwikkeling ervan, waardoor software zwakke plekken krijgt.

Het Duitse Federaal bureau voor informatiebeveiliging (BSI) kondigde aan dat "succesvolle aanvallen vaak het gevolg zijn van onbekende kwetsbaarheden en het ontbreken van patchbeheer."[3] De reden hiervoor is dat het aantal kritieke kwetsbaarheden in standaard IT-producten sterk is gestegen in de afgelopen jaren.

Alleen al in 2017 waren er meer dan 450 kwetsbaarheden bekend in de tien populairste toepassingen. Volgens het BSI zijn er geen aanwijzingen dat de situatie in de komende jaren zal veranderen. In 2019 werden er al 12.174 kwetsbaarheden geverifieerd in de top 50 meest gebruikte softwareproducten.4



Afbeelding 2: Kritieke CVE-vermeldingen vanaf 31-03-20185



Afbeelding 3: Verdeling van kwetsbaarheden in 2019 vanaf 30-10-2019. Van niet-kritiek (groen) naar kritiek (rood) van de top 504

90% van de benutte kwetsbaarheden in software verschijnen in de eerste 40 tot 60 dagen na de release. Aangezien IT-beheerders verantwoordelijk worden gehouden, moeten ze snel handelen. Patches moeten worden geïmplementeerd, getest en uitgerold. Dit kost IT-beheerders niet alleen ontzettend veel tijd, maar brengt ook een aanzienlijke kostenfactor met zich mee.

Door de stijging van het aantal kwetsbaarheden is handmatige patching nog tijdrovender en omslachtiger om op regelmatige basis te doen met de zekerheid dat alle apparaten ook daadwerkelijk succesvol zijn gepatcht. Handmatige patchingprocessen vereisen ook handmatige opvolgingsprocessen, waardoor extra druk wordt gelegd op de tijd en middelen van IT-beheerders.

Als het gaat om handmatige patchingprocessen, afhankelijk van de complexiteit van het systeem, kan het nodig zijn om patches te laten implementeren door eindgebruikers. Dit heeft doorgaans gevolgen voor de mate van succes van de patchimplementatie.

Patchen aan de kant van de server is relatief eenvoudig, omdat de IT-afdeling de volledige controle heeft. Echter, de meeste kwetsbaarheden (circa 95%) komen voor aan de clientzijde en het is moeilijk om clients up-to-date te houden. Logistieke problemen zoals de menselijke factor staan in de weg; mensen stellen patches uit omdat ze hun werk niet willen onderbreken. Om deze redenen wordt patchen vaak verzuimd; hoewel patches meestal lange tijd beschikbaar zijn, worden ze nooit geïmplementeerd door belemmeringen op het gebied van tijd en geld. Echter, als patches niet correct worden aangebracht, kunnen cybercriminelen stelselmatig misbruik maken van deze zwakke plekken.

Deze kwetsbaarheden in software kunnen leiden tot ernstige beveiligingsproblemen in een toepassing of IT-netwerk. Dit is de reden waarom bedrijven tegenwoordig voor de grote uitdaging staan van het beter organiseren en beheren van hun IT-infrastructuur. Patch Management is de optimale oplossing om IT-beheerders te ontlasten en de prestaties, efficiëntie en effectiviteit van de IT-infrastructuur te verbeteren. Een effectieve patchbeheeroplossing controleert welke patches het meest geschikt zijn voor de systemen, automatiseert de verdeling en uitrol van patches, en classificeert ze op basis van urgentie. Daarom verbetert patchbeheer niet alleen de implementatie van patches, maar beperkt het ook de handmatige stappen en het risico op menselijke fouten.

Risico's van ondermaats patchbeheer

Kostbare systeemonderbreking

Verlies van geloofwaardigheid bij klanten

Lange hersteltijd

Twijfelachtige gegevensintegriteit

Negatieve publiciteit

Onveilige IT-omgeving

Voordelen van patchbeheer

Regelmatige en geautomatiseerde patching verhoogt de beveiliging van IT-systemen en de integriteit van netwerken aanzienlijk. Dit is het meest voor de hand liggende voordeel van patchbeheer. Een geautomatiseerde

Verhoog de IT-productiviteit en beperk niet-geplande downtime

Handmatig patchbeheer is erg tijdrovend voor IT-beheerders. Kwetsbaarheden identificeren, bepalen welke eindpunten patches nodig hebben en ze uiteindelijk implementeren, en controleren of de patches correct zijn toegepast op de getroffen computers en laptops, kost veel tijd en middelen.

Bovendien veroorzaakt dit niet-geplande downtime voor werknemers die toegang tot hun apparaten nodig hebben. Een geautomatiseerde patchbeheeroplossing helpt daarom niet alleen het IT-personeel bij het verhogen van hun efficiëntie, maar beperkt ook de niet-geplande downtime voor werknemers.

Maakt naleving op het gebied van beveiliging en gegevens mogelijk om risico's te beperken

Richtlijnen voor naleving op het gebied van beveiliging zijn essentieel in IT-afdelingen en mogen niet worden onderschat. Naleving op het gebied van IT beschermt bedrijven tegen sancties of potentiële imagoschade. Zwakke plekken in software vormen bijvoorbeeld grote beveiligingsrisico's die kunnen leiden tot ernstige datalekken.

Als gevoelige gegevens van werknemers of klanten openbaar worden gemaakt, kunnen bedrijven sancties opgelegd krijgen voor het schenden van de wet- en regelgeving inzake gegevensbescherming. Dit kan leiden tot klantverloop of negatieve publiciteit. Een effectieve patchbeheeroplossing detecteert beveiligingsproblemen en kan helpen om deze risico's terug te dringen.

Belangrijkste **voordelen**

Bespaar tijd met snelle, alomvattende updates van het IT-systeem

Pas automatisch patches toe om zwakke plekken in software te herstellen

Beheer computers vanaf een centrale plek

Verhoog de productiviteit van werknemers

Benut inzichten uit gedetailleerde, net-werkoverschrijdende rapporten

Krijg inzicht in uw infrastructuur met systeemstatusover-zichten

Verminder niet-geplande downtime van apparaten

Beperk risico's op het gebied van beveiliging en naleving

Belangrijkste **eigenschappen**

Kwetsbaarheden identificeren

Krijg een volledig overzicht van uw netwerk door kwetsbaarheden als gevolg van verouderde software automatisch te detecteren.

Snelle uitrol, geïntegreerd met TeamViewer

Implementeer Patch Management met slechts enkele muisklikken in uw volledige

Automatische patchimplementatie

Detecteer en implementeer automatisch op beleid gebaseerde patches voor verouderde, kwetsbare software, besturingssystemen en toepassingen van derden om uw IT-infrastructuur veilig en up-to-date te houden.

De patchbeheeroplossing van TeamViewer

Het patchen van eindpunten kan uw volledige netwerk beschermen tegen cyberaanvallen. Maar wist u dat slechts één ongepatcht apparaat uw gehele IT-infrastructuur in gevaar kan brengen?

Met Patch Management van TeamViewer Remote Management **worden kwetsbaarheden automatisch gedetecteerd**, waardoor het eenvoudig is om elk apparaat up-to-date en veilig gepatcht te houden.

Bescherm uw IT-netwerken met Patch Management van TeamViewer

Houd kritieke patches nauwlettend in de gaten met geautomatiseerd patchbeheer. Zie direct of er updates beschikbaar zijn en installeer ze op grote schaal vanaf een centraal platform.

Houd al uw Windows-apparaten up-to-date door Windows-updates te beheren en installeren vanaf een centraal dashboard.

Beperk risico's: bewaak en implementeer automatisch patches voor toepassingen van derden en updates voor besturingssystemen.

Bekijk de patchstatus van uw apparaten en alle beschikbare patches op één dashboard.

Definieer afzonderlijke beleidsregels voor verschillende afdelingen of klanten om patchtaken aan te passen en te automatiseren.

Geef een prioriteit aan patches: zie welke patches kritiek of urgent zijn, en welke patches kunnen worden uitgesteld door ze te sorteren op prioriteit.

Beheer en controleer uw patches op afstand, ongeacht uw locatie. De naadloze integratie tussen TeamViewer Remote Management en TeamViewer Remote Access zorgt ervoor dat u met slechts enkele muisklikken toegang krijgt tot apparaten.

Conclusie

IT-organisaties weten dat ze hun bedrijven continu moeten beschermen tegen cybercriminelen en dat een geautomatiseerde patchbeheeroplossing essentieel is voor het verbeteren van de eindpuntbeveiliging. Hoewel patchbeheer zeer belangrijk is, hoeft het niet ingewikkeld te zijn.

Patch Management van TeamViewer heeft gebruiksvriendelijke functies waarmee u uw IT-infrastructuur proactief kunt beschermen en omslachtige handmatige patchingtaken kunt elimineren, terwijl de veiligheid, stabiliteit en integriteit van uw netwerk worden verhoogd.

Bronnen

Vraag een gratis demo aan van TeamViewer Remote Management (inclusief Patch Management)

Lees meer op teamviewer.com/patchmanagement

Ga aan de slag met een gratis proefversie van Patch Management

Referenties

1. National Institute of Standards and Technology (november 2019): Automation Support for Security Control Assessments: Software Vulnerability Management, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8011-4-draft.pdf
2. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf
3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=F64FE0EE50A281C976D952B395DCD531.2_cid369?__blob=publicationFile&v=5 S.11
4. CVE Details (2019): Current CVSS Score Distribution for all Vulnerabilities, https://www.cvedetails.com/cvss-score-distribution.php
5. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3 page. 43
6. CVE Details (2019): Vulnerabilities by Date, https://www.cvedetails.com/browse-by-date.php

Over TeamViewer

Als een wereldwijd toonaangevend platform voor connectiviteit op afstand stelt TeamViewer gebruikers in staat om verbinding te maken met iedereen en ieder apparaat, altijd en overal. TeamViewer biedt mogelijkheden voor veilige toegang, ondersteuning, beheer en samenwerking op afstand voor alle typen online eindpunten en ondersteunt bedrijven in alle soorten en maten bij het optimaal benutten van hun digitale potentieel. TeamViewer is geactiveerd op circa 2 miljard apparaten en er zijn tot 45 miljoen apparaten tegelijkertijd online. TeamViewer is opgericht in 2005 in Göppingen, Duitsland, en heeft een beursnotering op de Frankfurt Stock Exchange. Er werken ongeveer 800 mensen in kantoren overal in Europa, de VS en Azië-Pacific.

www.teamviewer.com