KAN DEZE PATCH VANDAAG NOG...?

SECURITY INTELLIGENCE

Microsoft heeft in haar Security Intelligence Report volume 18 (SIR) dat op 19 mei 2015 gepubliceerd is een analyse gemaakt van kwetsbaarheden in software, exploits en malware en zoomt daar in op de levenscyclus van een exploit. De conclusies van het rapport zijn niet mild en geven voor veel bedrijven voldoende stof tot nadenken.

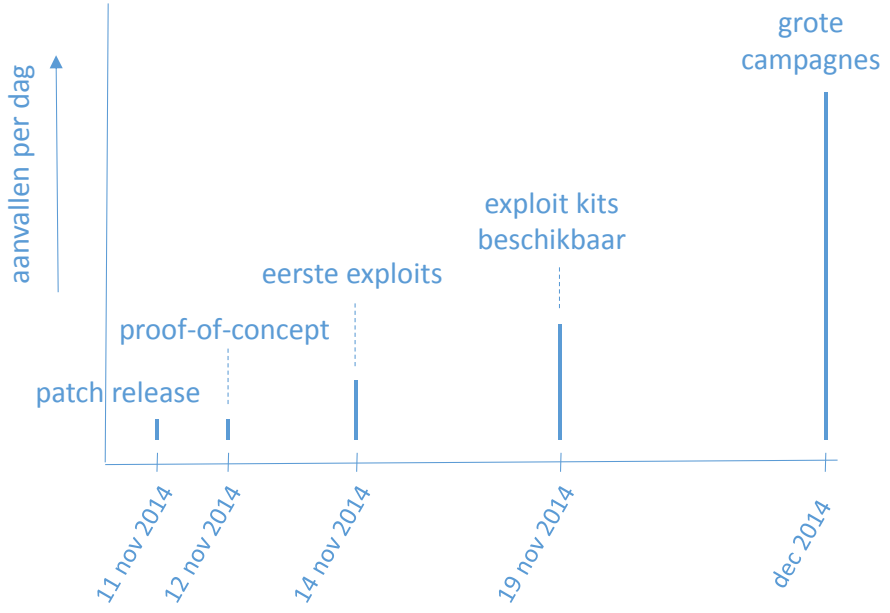
VAN PATCH NAAR EXPLOIT

Als voorbeeld hanteert Microsoft een patch die op 11 november 2014 uit is gekomen voor verschillende Microsoft producten. Deze is beschreven in het Microsoft Security bulletin MS14-064.

De dag na het uitkomen van de patch, 12 november, wordt door een onafhankelijke security onderzoeker in China een proof-of-concept exploit gepubliceerd.

Op 14 november constateert Microsoft dat de exploit al actief uitgebuit wordt op websites waar specifieke doelgroepen vaak komen. De zogenaamde *Watering hole* techniek.

Sinds 19 november is de exploit opgenomen in 'exploit kits' waarmee, onder andere door hackers, malware gebouwd kan worden. Op dat moment rapporteren er volgens het onderzoek al 1.500 computers per dag een poging om de exploit uit te buiten. Vanaf eind november stijgt dat aantal tot bijna 9.000 aanvallen per dag rond half december. Zelfs in maart 2015 worden de aanvallen nog waargenomen.



“VAN PATCH NAAR EXPLOIT BINNEN 1 DAG…!”

Volgens Gartner is Palo Alto Networks al jaren leider in Next Generation firewalls en scoort bij de *“NSS Labs’ 2015 Next Generation Intrusion Prevention System test”* op meerdere vlakken een 100% score.

SNEL PATCHEN

Veel bedrijven rollen een beschikbare patch niet meteen uit. Omdat het niet alleen om Microsoft patches gaat maar ook om netwerkapparatuur, virtualisatiesoftware en zeker ook applicaties zoals Acrobat Reader en webbrowsers, is het landschap aan dagelijkse updates en patches enorm. Het vooraf testen van patches kost tijd en er is niet altijd een service window beschikbaar voor een tussentijdse uitrol.

En toch kan een nog niet uitgerolde patch fataal zijn voor uw business. Hackers worden steeds professioneler en beschikken over vele tools om een uitgebrachte patch te analyseren en er een exploit voor te schrijven. Zelfs al binnen één dag.

ONZE AANPAK

Valid heeft hierop een passend antwoord. Patch Management gecombineerd met een Next Generation firewall van Palo Alto Networks, welke beschikt over Intrusion Prevention technologie.

Deze firewall ontvangt iedere 15 minuten updates waarmee nieuwe exploits gedetecteerd worden. Nog voordat een hacker uw server met een aanval bereikt heeft wordt deze door de Palo Alto Networks firewall herkend en tegengehouden.

Dat geeft de IT-afdeling de tijd om een beschikbare patch klaar te maken en uit te rollen, wat resulteert in tussentijds verhoogde bescherming.

Volgens een onderzoek van het Ponemon Institute waren de gemiddelde kosten van een data breach in Duitsland in 2014 €6.1M. Goede preventiemaatregelen kunnen u een hoop geld besparen.

Daarnaast biedt de Palo Alto Networks firewall nog vele andere voordelen. Denk aan zaken zoals de detectie van virussen en spyware, het blokkeren van drive-by downloads en geautomatiseerde bedreigingenanalyse van onbekende applicaties.

INTERESSE?

Wilt u meer weten over de mogelijkheden die Valid te bieden heeft op het gebied van Patch Management en de Next Generation technologie van Palo Alto Networks, neem dan contact op met:

Nico Kleijnen
Manager Infrastructures
+31 (0)88 – 900 9500

Flight Forum 565, 5657 DR Eindhoven
www.valid.nl