Ransomware aanval _

velzart.nl/blog/ransomeware/

July 5, 2021

Update: 16:15 uur – 16-07-2021

2 juli 2021 18:32 uur, een datum en tijd om nooit te vergeten, of misschien toch wel…

Vandaag, 16 juli, exact twee weken na de welbekende ransomware aanval volgt hier onze laatste reguliere update omtrent dit onderwerp.

Onze collega's Arno en Cristian zijn bezig met het afronden van de laatste werkzaamheden bij een klant. Een klant van het eerste uur waar wij server en patchkast werkzaamheden hadden uitgevoerd. Arno merkte een enorme vertraging op zijn laptop. herstartte zijn systeem en zag direct op de server ook rare zaken gebeuren. Cristian kwam om de hoek met de fameuze woorden: "Uh Arno, gaat dit goed? ". Monitoringsystemen slaan rood uit, klanten bellen met de storingsdienst en accountmanagers en de VelzArt 24/7 groepsapp knalt bijna uit elkaar. Het begin van twee bewogen weken.

De updates die we de afgelopen weken hebben gedaan geven een goed beeld van de verhaallijn tot nu toe. Deze week zijn we druk bezig geweest om alle lopende zaken tot een goed einde te brengen. Met nog een twintigtal tickets waarvan met de meeste klanten inmiddels contact is geweest gaan wij tevreden het weekend in.

Het mag duidelijk zijn dat alle positieve zaken die we melden relatief zijn. De hele situatie, die ontstaan is door een aantal Russische criminelen, hadden we liever niet gezien. We hadden het liever anders gezien maar zijn omgegaan met de feiten die voor ons lagen. Anderhalf uur na de uitbraak waren we servers aan het restoren. Vrijdagnacht hebben we

nog 10 servers van diverse locaties opgehaald om naar Waardenburg te brengen. We hebben nachtdiensten gedraaid om 24 uur per dag operationeel te zijn, 5 dagen lang. We hebben 100% van de servers kunnen herstellen! En exact 2 weken na de uitbraak zijn we er weer, in volledige controle.

Deze week zijn we gestart met de verschillende evaluaties en onderzoeken. De oorzaak, het gevolg en het uiteindelijke proces tot de dag van vandaag gaan we bekijken. Onze mensen hebben echt keihard gewerkt en we zijn dan ook meer dan trots, op een ieder. Hebben we alles feilloos gedaan? Zeker niet. Zoals een collega deze week zei: "*Waar gehakt wordt vallen spaanders*". We zullen in ieder geval alles in het werk stellen om hier samen met onze klanten nog sterker uit te komen! We zien de toekomst met een (glim)lach tegemoet.

De bedankjes zijn in de afgelopen updates al voorbij gekomen en dit kunnen we niet genoeg doen. Onze klanten, onze partners, collega-bedrijven, vrienden, familie, ex-collega's, en geïnteresseerde bedankt.

Het laatste bedankje (en wellicht een klein excuusje hier en daar) gaat echter naar onze partners en kinderen!

"De zon schijnt weer dit weekend, wij ook, tot zo ! ♥"

Update: 20:45 uur – 13-07-2021
Volgende update einde week 28.

Vanwege het ontbreken van nieuws zal onze volgende update zijn richting het einde van deze week 28.
Mochten er vragen zijn kunt u terecht via de gebruikelijke kanalen.

Update: 21:10 uur – 12-07-2021
Volgende update dinsdag richting de avond, de laatste update (voorlopig).

Een korte update voor de maandagavond.

Zoals bekend hebben we dit weekend de spreekwoordelijke batterijen weer opgeladen. Voor een aantal klanten hebben we nog wat punten op de i kunnen zetten dit weekend en ook wat voorbereidingen kunnen treffen voor deze week. De planning stond vanochtend weer vol en iedereen kon weer, binnen en buiten, aan de slag.

Op technisch vlak hebben we op dit moment geen verdere updates dan wat afgelopen week is gemeld. Deze week hopen we alle punten af te kunnen ronden rondom de ransomware aanval. Gelukkig kunnen we melden dat van alle klanten tot 5 werkplekken er slechts 30%

getroffen is door de aanval. Dit blijft voor de getroffenen uiteraard enorm vervelend echter had dit dus nog vervelender uit kunnen pakken, voor veel meer bedrijven / mensen.

Morgen zullen we onze voorlopig laatste update doen vanuit dit onderwerp. Mocht er nieuws zijn uit de hoek van Kaseya, bijvoorbeeld in de vorm van een key, of andere belangrijke zaken dan melden we ons uiteraard direct. Overige updates zullen we in persoonlijke vorm bespreken met klanten die het betreft.

Update: 14:30 uur – 10-07-2021
Volgende update maandag omstreeks 18.00 uur.

Een extra update op zaterdag 10 juli.

Waarschuwing

Afgelopen vrijdag is er wereldwijd een ransomware aanval gelanceerd waar enorm veel bedrijven én privé personen slachtoffer van zijn geworden. Zo ook VelzArt en zo ook klanten van VelzArt. De ervaring leert dat na een aanval van deze omvang er weer andere criminele bendes volgen die ook een graantje willen meepikken. Helaas is dit ook de realiteit. Via deze berichtingeving willen we dan ook een ieder waarschuwen voor hetgeen wellicht komen gaat.

- **Spam e-mail**: Er kan mail rondgestuurd worden met daarin een programma, een link of een verwijzing naar een website waar de oplossing mogelijk zou staan. Er is geen fix voor de problematiek met Kaseya. Er is geen oplossing ondanks dat we dit allemaal graag zouden willen. Is deze er wel dan zullen wij u hierover informeren via onze eigen kanalen. Vertrouw dit soort mailtjes niet!
- **Telefonisch**: Er gaan mogelijk Engels of Nederlands sprekende mensen rond bellen vanuit Microsoft of Kaseya, althans zo doen ze zich voor. Ze willen meekijken met de computer om het probleem op te lossen. Ook dit is onzin, dit bestaat niet! Vertrouw dit absoluut niet.
- **In persoon**: Er is altijd wel een bekende van een neef van de buurman die ook de oplossing kan bieden, voor een x-bedrag. Met een herinstallatie kan een dergelijk persoon wellicht helpen maar met een fix voor de encryptie op de bestanden écht niet.

Uiteraard staan onze spamfilters scherp om bepaalde e-mail tegen te gaan maar bijvoorbeeld op privé e-mail hebben wij natuurlijk geen controle. Wees waakzaam, zorg dat de mensen rondom u heen ook goed opletten. Met een week of 2 á 3 zal ook deze storm gaan liggen echter waakzaamheid (awareness) rondom ICT is echt enorm belangrijk.

Fijn weekend.

Update: 16:10 uur – 09-07-2021
Volgende update maandag omstreeks 18.00 uur.

De laatste update van week 27, een week die we niet snel zullen vergeten…

Politie aangifte

Vandaag zijn we in contact gekomen met het Cybercrimeteam van de politie Oost-Nederland. In samenwerking met dit team gaan we onze aangifte de komende week verder compleet maken. Het onderzoek zal vandaaruit gestart worden, in samenwerking met het Team High Tech Crime van de politie en de FBI. Deze laatste (klinkt bijna alsof we in een (slechte) film zitten) schijnt redelijk ver te zijn met hun onderzoek.

De vraag of klanten van VelzArt ook aangifte moeten doen is ook direct beantwoord: dit hoeft niet, al staat iedereen hier vrij in. De extra aangiftes van klanten betekent alleen meer extra werk voor de politie en draagt niet extra bij aan het onderzoek.

Status tot nu toe

Uit eerdere updates mag blijken dat we veel werk hebben verzet. Vandaag ook hebben we met onze mensen weer alles gegeven. We hebben zeker nog net met iedereen contact gehad, ondanks dat we dit graag ook geregeld hadden. We zullen hier komende week weer vol gas op moeten geven. Dat gaan we ook doen uiteraard.

Wel kunnen we ook melden dat alle back-ups van de klanten met ENOA – backup & controle voor 100% geslaagd zijn en dus gedraaid hebben. De ervaring leert hoe belangrijk deze zijn.

Weekend

Even de balans opmakend kunnen we stellen dat veel van onze mensen inmiddels richting het einde gaan van de 12e achtereenvolgende werkdag. Dit is dan los gezien van alle lange dagen en nachtelijke uren. We hebben dan ook besloten om een normaal weekend voor iedereen in te lassen. De batterijen moeten echt opgeladen worden.

Als laatste willen we iedereen bedanken. Onze klanten, leveranciers, collega bedrijven inclusief extra dank voor de mannen die ons geholpen hebben op klantlocaties, de software leveranciers van diverse klanten, de lokale bakkers, onze partners thuis inclusief alle toegeschoten oppashulpen en uiteraard onze mensen zelf!

Eén van onze ingeleende krachten van een collega bedrijf refereerde gisteren aan ‘de bijzondere sfeer onderling, ondanks de problemen en ondanks de enorme hoeveelheid gewerkte uren’. Hier sluiten we mee af. Het was een bijzondere week. Maandag gaan we weer met hernieuwde energie aan de slag. We zijn trotse VelzArdianen!

Goed weekend.

Update: 18:03 uur – 08-07-2021
Volgende update donderdag omstreeks 18.00 uur.

De korte update van de donderdag, 8 juli 2021.

Zoals gemeld gisteren lopen de herstelwerkzaamheden op klant locatie goed door. De buiten- en binnendienst ploegen geven alles om zoveel als mogelijk klanten weer up and running te krijgen. Dit proces zal uiteraard ook morgen weer ‘gewoon’ plaats vinden.

Politie aangifte

Morgen hebben we een afspraak staan met de politie om daar aangifte te doen van hetgeen gebeurd. Tijdens deze afspraak zullen wij ook nagaan wat er wordt verwacht van onze klanten in deze. Een collectieve aangifte, een individuele aangifte middels een bepaald format of geen aangifte omdat wij als VelzArt zijnde dit al hebben gedaan en de casus duidelijk is. Hier zullen we dus later op terug komen.

Een kort overzicht van de klantsituaties op dit moment.

Categorie	Inname	Recovery	Terugplaatsing
Servers on-premise	100%	100%	100%
Werkplekken gekoppeld aan servers on-premise	100%	100%	100%
Cloud servers	NVT	100%	NVT
Werkplekken gekoppeld aan cloud server	100%	100%	100%
Werkplekken met back-up	100%	100%	100%
Losse werkplekken	40%	35%	30%

De volgende update zal morgen, vrijdag 9 juli zijn, omstreeks 16.00 uur.

Update: 10:45 uur – 08-07-2021
Volgende update donderdag omstreeks 18.00 uur.

Een kort extra update op de donderdagochtend, 08-07-2021 om 11.00 uur.

Dataverlies
Herinstallatie van een computersysteem betekent dat alle data en software wordt verwijderd. Software is uiteraard gewoon opnieuw te installeren, er vanuit gaande dat de licenties aanwezig zijn. Data is helaas een ander verhaal. Is er geen back-up van het systeem dan gaat de data verloren.

Bestaat er géén kans dat data hersteld kan worden?
Jawel, er bestaat een kans dat data hersteld kan worden, een hele kleine kans. Bij eerdere ransomware aanvallen van formaat is gebleken dat er in sommige gevallen uiteindelijk een key komt die de versleuteling ongedaan kan maken. Of deze key er komt én op welke termijn is op dit moment niet duidelijk. Gezien het feit dat er veel bedrijven in een land als bijvoorbeeld Amerika zijn getroffen doet ons hopen hierop, maar wellicht wel tegen beter in. Wij weten het ook niet in deze, helaas.

Om deze 'kans' ooit te kunnen verzilveren bestaat er de optie om de data die versleuteld is te bewaren. De huidige harde schijf van het computersysteem zullen we in deze gevallen vervangen voor een nieuwe SSD harde schijf. Het computersysteem zal opnieuw worden geïnstalleerd op de nieuwe SSD harde schijf. De oude harde schijf kan worden bewaard totdat over de key meer nieuws is. Nogmaals, of en wanneer we hier iets mee gaan kunnen zal later blijken.

Deze optie kan besproken worden met onze medewerkers wanneer we contact opnemen over de betreffende computersystemen.

Tot zover deze update, richting het einde van de dag melden wij ons weer.

Update: 19:30 uur – 07-07-2021
Volgende update donderdag omstreeks 18.00 uur.

Vandaag wint Wout van Aert een heroïsche etappe in de Tour de France met hierin maar liefst twee beklimmingen van de Mont Ventoux. Deze prachtige berg heeft twee kanten om naar boven te gaan, een hele steile kant en de ietwat makkelijkere / flauwere kant. Vandaag, richting het einde van de dag, voelt het alsof we de eerste steile kant met succes hebben beklommen. We hebben niet gewonnen, dat mag duidelijk zijn, maar dat we met zoveel kracht toch boven zijn gekomen voelt wellicht wel in die richting. De komende dagen zullen we uiteraard ook volle bak aan de slag gaan om ook via de andere kant boven te komen!

Vandaag hebben we de laatste servers met succes teruggeplaatst, op één data back-up na (we moeten eerlijk zijn) is dat gedeelte afgerond. Een eerste grote groep klanten zijn daarnaast door diverse buiten- en binnendienst mensen weer volledig operationeel gemaakt. De komende dagen gaat dat ook het doel zijn, iedereen weer volledig operationeel krijgen.

Vanavond is ook de eerste nacht dat er geen activiteiten meer zullen zijn op de Ringweistraat. Alle werkzaamheden zullen vanaf heden op klant locatie worden uitgevoerd, of remote.

Een korte technisch update:

Bescherming na herinstallatie Windows 10

Een oplettende klant stelde ons de vraag: is mijn systeem wel beschermd voor virussen, na een complete herinstallatie. Het antwoord op de vraag is: ja! Windows 10 wordt standaard geïnstalleerd met Windows Defender, een prima eerste bescherming totdat wij onze ENOA dienstverlening compleet hebben uitgerold. Hiermee lopen we overigens ook goed volgens planning, dit moet voor het weekend zo goed als afgerond zijn.

Bedankjes hebben we de afgelopen dagen meerdere malen uitgedeeld. Deze keer een mededeling van de verschillende ambachtelijke bakkers in de regio Waardenburg: de slagroom is op! Het is niet te geloven hoeveel heerlijke taarten we de afgelopen dagen hebben mogen ontvangen. Onze mensen komen iedere dag oprecht vermoeid thuis maar hebben in ieder geval een heerlijk vol buikje. Dank!

Morgen gaan exact dezelfde ploegen weer op pad, inclusief externe hulp. Intern hebben we dezelfde opstelling als vandaag en gaan we volle bak aan de slag om iedereen weer verder te helpen. Onze mensen zullen ook weer volop klanten informeren en updates opvragen over de huidige status. Het verzoek blijft in deze hetzelfde als de afgelopen dagen: wij nemen contact op. We weten dat er nog veel klanten zijn die écht nog niet operationeel zijn. Werkstations die nog niet gereed zijn, software pakketten die niet werken en data die verdwenen is. Het is absoluut ook ons een doorn in het oog. We proberen een positieve boodschap uit te stralen om ook onze eigen moraal hoog te houden maar we zijn ons bewust van de realiteit. We gaan ervoor mensen, jullie staan er niet alleen voor!

Morgen zullen we wederom updaten richting het einde van de dag, tenzij er uiteraard iets waardevols tussendoor te melden is.

Extra update: 11:30 uur – 07-07-2021
Volgende update donderdag omstreeks 18.00 uur.

Een korte update op deze woensdagochtend aangaande Microsoft Office 365.

We zijn in de gelukkige omstandigheid dat veel van onze klanten gebruik maken van een Cloud licentie van Microsoft 365. In eerdere berichtgevingen is al meegenomen dat deze omgevingen schoon zijn gebleven van de aanval. Microsoft heeft herkend dat de aanval er was en heeft de laatste versies van alle bestanden hersteld. De conclusie is dan ook dat mensen in de Cloud door kunnen werken.

Werken in de Cloud
Zoals ook eerder aangegeven kunnen mensen die werken via Microsoft 365 inloggen op https://office.com. Via de online omgeving kan toegang worden gekregen tot Outlook voor de e-mail maar bijvoorbeeld ook SharePoint. Links bovenin ziet u, na inloggen, een kubus met stippen waar u toegang kunt krijgen tot alle apps.

Installeren van Office
Na het herstellen van een Windows installatie zal ook Office (Microsoft 365) opnieuw geïnstalleerd moeten worden. Ga naar https://portal.office.com. Na het inloggen ziet u een begroeting (Goedemorgen / Goedemiddag) waar rechts van u de knop “Office installeren” zult zien. Hier kunt u de Office 365-apps downloaden voor lokaal gebruik. Normaliter kunt u na het downloaden / installeren en verificatie met alle apps direct aan de slag.

Tot zover deze update, richting einde werkdag zullen wij ons wederom melden.

Update: 19:30 uur – 06-07-2021
Volgende update woensdag omstreeks 18.00 uur.

De dinsdagavond update!

De laatste herstel procedures van fysieke servers lopen en zullen omstreeks middernacht afgerond zijn. Redelijk volgens planning en in ieder geval tot opluchting van ons en onze klanten. Deze laatste servers zijn in deze dan ook ‘de zware jongens’. Denk hierbij aan enorme hoeveelheden data, complexe inrichtingen en koppelingen met diverse externe bronnen. Het herstel van deze kolossen is een complexe materie die veel tijd kost. Morgen zullen we dus ook de laatste servers op diverse klantlocaties terug plaatsen. Het herstel van werkstations met back-ups loopt inmiddels ook behoorlijk door dus hier gaan we morgen ook weer terug afleveren bij onze klanten.

Vandaag hebben we onze Servicedesk opgeschaald met o.a. steun van onze eigen Administratie om in ieder geval iedereen te woord te kunnen staan. Een deel van onze Servicedesk is daarmee achter de eigen werkplekken gekropen om ondersteuning te bieden bij klanten met issues op server- of werkplek gebied. De komende dagen zal deze opstelling zo blijven en verwachten we ook daar meters te kunnen maken.

Morgen zullen we in de loop van de dag met verschillende ploegen, in setjes van twee personen, weer op pad gaan om op klant locaties de laatste punten op de i te zetten. Deze setjes zijn vaak wederom opgebouwd uit een medewerker van VelzArt en één van een collega bedrijf. Deze samenwerking bevalt ons, ter info, buitengewoon goed. We zijn echt geholpen met enorm vakkundige mensen. Daarnaast zal een vliegende keep op pad worden gestuurd om werkstations weer terug te brengen op locatie en ook diverse systemen weer op te halen. We zullen ook in sommige gevallen beroep doen op klanten om zelf ook

machines te brengen en halen, in overleg uiteraard. Al met al zijn er morgen weer 40 mensen onderweg of werkzaam vanuit Waardenburg om iedereen weer aan het werk te krijgen.

Tijdens het avond eten zojuist werden de urenstaten van een ieder voor deze week met een lach besproken. De zomervakanties komen voor een ieder in één keer rap dichterbij 😊. Met een serieuze noot: het energielevel van sommige moet weer even opgepoetst worden en dus hebben we een groot gedeelte van onze mensen inmiddels huiswaarts gestuurd om vannacht goed bij te slapen. Morgen wacht weer een belangrijke dag waar we met z'n allen weer met volle energie in stappen.

Deze update is direct de laatste van vandaag. Morgen zullen we richting het einde van de dag ons wederom melden, tenzij er eerder nog nieuwswaardigheden te benoemen zijn uiteraard.

Voor nu een fijne avond!

Update: 11:30 uur – 06-07-2021
Volgende update dinsdag omstreeks 18.00 uur.

Dinsdagochtend, de tweede reguliere werkdag, de update van 11.30 uur.

Onze nachtploeg is inmiddels het bed in gedoken en de dagploeg is actief. We hebben de capaciteit van onze Servicedesk opgeschaald om zoveel als mogelijk mensen te woord te staan. Een ander deel van onze Servicedesk is op dit moment bezig om zoveel als mogelijk issues bij klanten op te pakken.

Zoals aangegeven in de update van gisterenavond zijn we op dit moment druk bezig met de laatste server situaties qua herstel om de buitendienst weer op pad te sturen voor herplaatsing op locatie. De verwachting is om tegen middernacht de laatste servers fysiek hersteld te hebben om deze morgen op locatie terug te plaatsen. Na afronding hiervan zal onze volledige focus liggen op de werkstations en lokale applicaties bij onze klanten. Gezien de grote aantallen verwachten wij hier zeker tot aan het weekend mee bezig te zijn.

Inmiddels hebben we mensen ook onderweg om diverse werkstations inclusief back-up op te halen om ook hiervan het herstel te starten. Na contact met onze teams hebben ook een aantal klanten inmiddels de werkstations terug gebracht. Hierbij direct het verzoek: retour werkstations richting VelzArt ALLEEN in overleg met onze afdelingen. Dit in verband ook met de veiligheid van uw eigen data. We proberen ook hierin de juiste prioriteiten te stellen.

De volgende update zal zijn omstreeks 18.00 uur.

Update: 17:40 uur – 05-07-2021
Volgende update dinsdag omstreeks 11.00 uur.

De maandag update van 17.30 uur, de eerste reguliere werkdag na de ransomware aanval.

We zijn (relatief) blij om te melden dat we inmiddels 70% van alle serversituaties technisch hebben hersteld en dat deze retour zijn richting klant of dat dit in ieder geval in de planning staat. De verwachting is dat de laatste servers vannacht de 'bank' op gaan om hersteld te gaan worden en richting dinsdagavond en/of woensdagochtend teruggeplaatst kunnen worden. Uiteraard met de kanttekening dat alles goed door blijft lopen. Alle klanten waar het betrekking op heeft zijn op de hoogte.

Dinsdag starten we met het verzamelen van de werkstations, die voorzien zijn van een back-up optie, om deze te gaan herstellen. Vanaf woensdag hopen we de planning rond te maken om ook te starten met de werkstations, die inmiddels een herinstallatie hebben gehad, om deze verder op te nemen in de bedrijfsnetwerken en/of functioneel te maken. Ook hierin zullen we nader in contact treden met onze klanten op het moment dat het van toepassing is.

Zonder in herhaling te vallen, maar toch nogmaals goed om te benoemen: de steun van o.a. collega bedrijven Aspect ICT uit Hardinxveld-Giesendam, Verdel ICT & Media uit Roelofarendsveen en IT Creation uit Papendrecht en en diverse bevriende ICT engineers, die ons ook de komende dagen zullen ondersteunen, is gigantisch. Nogmaals, het doet ons goed. Dank aan een ieder, voor welke bijdrage dan ook. We zullen hier later uiteraard meer aandacht aan besteden.

In diverse media is onze naam de afgelopen dagen genoemd of zijn we zelfs fysiek in beeld geweest. Ondanks de drukte en het feit dat 'de pet er niet toe stond' heeft één van onze directeuren Wesley Born een kort interview gegeven bij RTL Nieuws. De boodschap van verslaggever Marcel Maijer van RTL was eigenlijk, geef een interview of wij maken ons eigen verhaal, wat feitelijk gezien natuurlijk ook waar zou gaan zijn. Het interview was daar en achteraf moeten wij zeggen dat het interview, uit het hart, een juiste weerspiegeling is van de timeline waarin wij ons hebben begeeft tot afgelopen zaterdag omstreeks 18.00 uur. Met toestemming van RTL hebben wij het bericht op onze website geplaatst welke te vinden is via deze link: https://velzart.nl/blog/interview-rtl/

We hopen met de publicatie van dit interview veel vragen van mensen rondom ons te beantwoorden en een goed beeld te geven van de wereld waar wij ons tot op zaterdag in hebben begeeft. Verdere contacten met de media lopen. We zullen hier zeer beperkt in naar buiten treden.

Onze mensen zullen ook deze nacht weer aan de slag zijn met herstel werkzaamheden. We verwachten geen technische verandering meer deze dag, anders dan op individueel niveau. Om deze reden is dit de laatste update van vandaag en melden wij ons weer morgen omstreeks 11.00 uur.

De laatste noot is een bericht aan onze klantenkring, komend vanuit ons voltallige personeel: Dank!

We zijn de afgelopen dagen overspoelt met heerlijke versnaperingen, lieve berichten maar bovenal begrip en constructieve bijdrages. Ons team Service en Sales heeft ontzettend veel contacten gehad de afgelopen dagen via mail, telefoon, WhatsApp en uiteraard op locatie. Het begrip voor de ontstane situaties en het meewerkende karakter om bijvoorbeeld 'te helpen sjouwen' of systemen te her-installeren is ongelooflijk. Tijdens gesprekken met potentiële medewerkers en/of klanten heb je het wel eens over 'een warme band' hebben met klanten, iets waar wij natuurlijk altijd voor gaan. Om dat op dit moment, in deze situatie, te ervaren is bijzonder en hartverwarmend waarvoor nogmaals onze uitdrukkelijke dank, van iedereen.

Voor nu een fijne avond.

Update: 11:30 uur – 05-07-2021
Volgende update maandag omstreeks 17.00 uur.

De maandagochtend update van 11.30 uur, de dag dat iedere klant weer richting zijn/haar kantooromgeving is getrokken. Gelukkig zijn er ook een groot aantal klanten die voor een groot gedeelte of zelfs volledig gevrijwaard zijn van problemen. Een positieve noot in ieder geval. Uiteraard worden wij als organisatie veel benaderd voor specifieke vragen, welke wij ook naar eer en geweten zullen beantwoorden. Ondanks de druk en ondanks het in veel gevallen het moeten brengen van slecht nieuws wordt de boodschap door onze klanten veelal met begrip en toekomst gerichte visie aangenomen. Onze dank hiervoor!

De verschillende varianten van het virus, of althans de verschillende varianten van het resultaat ervan doen veel vragen oproepen. Om deze reden nog een korte uitleg.

Readme txt: dit bestand is eigenlijk het eindresultaat van het virus en is normaliter terug te vinden op het bureaublad. De naam van het bestand wordt voorafgegaan door een random aantal cijfers dus bijvoorbeeld 304949_readme.txt. Dit is eigenlijk het bestand waarin aan wordt gegeven door de hackers hoe en hoeveel losgeld betaald kan worden.

Mpsvc.dll: dit bestand is terug te vinden in de directory C:\windows. Dit is het bestand wat de oorzaak is van de uiteindelijke encryptie van de bestanden. Dit bestand heeft er uiteindelijk voor gezorgd dat de encryptie en het readme bestand zijn gegenereerd.

Kaseya software: deze software heeft afgelopen vrijdag gezorgd voor de distributie van bovenstaande dll bestand richting de computers en servers. Alle connecties met de software van Kaseya zijn vrijdagavond omstreeks 19:30 uur verbroken en dus kan verdere distributie niet meer plaats vinden. Is er nu niets gebeurd op het systeem dan gaat het ook niet meer gebeuren.

Werkplekken: op het moment dat op een werkstation (laptop / desktop) nu geen readme bestand op het bureaublad én bestanden op het bureaublad, de map downloads en mijn documenten gewoon te openen zijn is het computersysteem niet besmet. Werken op deze stations kan gewoon gebeuren zoals normaal. Zijn bestanden niet benaderbaar dan zal een herinstallatie van het systeem, met daarbij verlies van lokale bestanden en software, een jammerlijk gevolg zijn. Zelf het systeem resetten kan uiteraard, kijk voor dit proces op https://velzart.nl/reset.

Ons team Service en Sales probeert maximaal in contact te komen met klanten indien dit van toepassing is. Ook na herinstallatie zijn er uiteraard nog voldoende handeling om te komen tot een volwaardige werkplek. Helaas kunnen wij daarin niet iedereen per direct begeleiden. We hopen ook hier op uw begrip en begrijpen dat dit een zware last is. De boodschap blijft helaas wel: wij zullen contact met u opnemen! Wil u uw problematiek ons kenbaar maken, geef dan uw update aan via https://velzart.nl/update. Zodoende zult u ook worden meegenomen in de verdere berichtgeving, mocht dit niet al het geval zijn.

Update: 22:30 uur – 04-07-2021
Volgende update maandag omstreeks 11.00 uur.

Zondagavond 22.30 uur, de laatste update van vandaag.

Servers – het allergrootste gedeelte van servers van onze klanten is hier op locatie en/of inmiddels weer retour richting klant locatie. Ook deze nacht gaat er weer een team volop de werkzaamheden doorzetten om morgenochtend maximaal server situaties richting de klant terug te kunnen brengen. Ondanks de maximale inzet is het wel eerlijk om aan te geven dat we zeker niet alle klanten hierin kunnen bedienen maar de klanten die het betreft zijn inmiddels ook op de hoogte.

Werkstations – Deze middag en avond hebben we via ENOA een script laten lopen om de impact van de situatie goed in te kunnen schatten en daar waar mogelijk systemen op te kunnen schonen van de initiële bestanden van de aanval. De bron van de software is sinds vrijdagavond al niet meer actief. Deze twee zaken zorgen ervoor dat we voor werkstations meer duidelijkheid hebben.

Vanaf dit moment gelden de volgende zaken:

- Heeft het computersysteem vandaag aangestaan, verbonden aan het internet, dan heeft ENOA inmiddels zijn werk gedaan. Login op het computersysteem. Controleer of er op het bureaublad een readme txt bestand staat. Is dit niet zo, controleer dan of lokale excel en/of word bestanden toegankelijk zijn. Kunnen deze bestanden gewoon worden geopend dan is het systeem niet besmet.

- Heeft het computersysteem niet aangestaan, zet het systeem dan aan, verbonden met het internet. Wacht minimaal een half uur met iedere verdere actie, log dus niet in. Geef ENOA even de tijd om het systeem op te schonen. Na een half uur kan vervolgt worden met de stappen hierboven.

Is de toegang tot bestanden op de computer verhinderd dan is het systeem besmet. Het systeem zal moeten worden hersteld. Wilt u zelf over gaan tot herstel van het systeem dan kunt u kijken op https://velzart.nl/herstel voor de procedure.

We hebben diverse vragen gekregen over datalekken door de ransomware aanval. Uit diverse bronnen uit de gehele wereld blijkt dat het hier niet gaat om het stelen van data, maar puur om het gijzelen van data om losgeld te krijgen. Dit ter info.

Deze zondagavond willen we graag afsluiten met een positieve noot. Zoals eerder gemeld hebben we uit diverse hoeken van collega bedrijven hulp aangeboden gekregen. In deze tijden waar we toch wat zwaarmoedig tegen de wereld aan kijken is dit toch wel een buitengewoon lichtpuntje. De aandacht van collega's, de gebaren, de berichten zijn een groot hart onder de riem van ons complete team. De handreiking van diverse collega's hebben we ook meer liefde aangenomen en zo hebben we vandaag en gisteren de eerste versterkingen mogen ontvangen en zal ons team ook morgen worden versterkt met diverse krachten. Nogmaals onze uitdrukkelijke dank, aan iedereen.

De dag van morgen staat voor ons in het teken van het afleveren en herstellen van de laatste serversituaties. Daarnaast gaan we direct aan de slag met de planning voor alle besmette werkstations om in de loop van de dag ook daar meer inzicht over te kunnen geven. De eerder verstuurd boodschap blijft van kracht, wij komen graag in contact met klanten maar laat het initiatief in deze zoveel mogelijk bij VelzArt liggen.

Update: 17:15 uur – 04-07-2021
Volgende update omstreeks 22.00 uur.

De beloofde zondag update van 17.15 uur. Allereerst enorme dank aan alle klanten die hun zondagse activiteiten enigszins hebben gepauzeerd om ons te helpen. Het aanzetten van alle computersystemen geeft ons meer inzicht in de impact van de aanval. We zijn op dit moment nog druk bezig om middels ENOA alle facetten te belichten en op te lossen daar waar mogelijk. De huidige bezetting van ons team zorgt ervoor dat we op dit moment nog niet zover zijn als we zelf zouden willen, ten aanzien van het proces rondom de werkstations. We verwachten hier in de loop van de avond meer resultaten.

Organisaties waarvan de systemen aan staan en waar we goed inzage hebben in de gevolgen zullen we trachten vanavond persoonlijk nog te berichten, telefonisch of via de mail. Ons doel is om daar waar wij informatie hebben deze ook te verstrekken. Ons verzoek

blijft hetzelfde: schakel zoveel als mogelijk computersystemen in, verbonden met internet. Wij gaan met deze systemen nog aan de slag.

Voor systemen waarvan inmiddels de conclusie is getrokken dat ze besmet zijn kan gestart worden met de reset procedure, https://velzart.nl/reset. Dit betekent feitelijk gezien een complete herinstallatie van het systeem waarbij data en software verloren zal gaan. Mocht u zelf aan de slag willen gaan, lees dan de procedure goed.

Voor veel mensen is dit standaard, maar bijzonder genoeg geldt dit voor ons ook, we hadden gehoopt dat dit weekend langer zou duren. Dit is uiteraard niet zo en dus staat de eerste werkdag van de week, de maandag, voor de deur. Belangrijke boodschap: deze komende week zal ons pand niet toegankelijk zijn. We zullen ons terrein afgrendelen van de buitenwereld om rust te creëren voor onze mensen én om de veiligheid van data van onze klanten te garanderen. De boodschap mag dan ook duidelijk zijn: kom niet naar VelzArt in Waardenburg, tenzij anders is afgesproken. Een bijzondere tijd vraagt helaas in deze ook om bijzondere maatregelen.

Een korte herhaling van bovenstaande: we zijn druk bezig met alle werkzaamheden. We gaan vanavond nog zoveel als mogelijk communiceren naar klanten, daar waar duidelijkheid is over de huidige situatie. Wij treden in contact met u als klant, probeer zoveel als mogelijk ons te ontlasten, ook de komende dagen. Meld uw situatie aan via https://velzart.nl/update indien dit nog niet is gebeurd. Kom niet naar VelzArt, tenzij anders is afgesproken.

De laatste update van vandaag zal omstreeks 22.00 uur volgen.

Update: 14:00 uur – 04-07-2021 (BELANGRIJK)
Volgende update omstreeks 17.00 uur.

Deze keer een zeer korte en duidelijke update voor alle werkstations, mogelijk geïnfecteerd met de ransomware. Wij willen iedereen met een werkstation verzoeken om deze per direct (zo snel als mogelijk) aan te zetten, met verbinding met internet. **LET OP**: het gaat hier puur en alleen om het aanzetten van het werkstation! **LOG NIET IN!** Geen verdere handelingen, geen controle, geen ‘even kijken’, niets!.

We hebben deze ochtend gewerkt aan een automatiseringsslag om systemen automatisch te controleren en daar waar mogelijk op te schonen. Dit gaan we in de komende uren uitvoeren. Opvolging van dit bericht zal volgen omstreeks 17.00 uur!

Nogmaals het verzoek om per direct (zo snel als mogelijk) alle computersystemen aan te zetten en (herhaling) NIET IN TE LOGGEN.

Update: 11:20 uur – 04-07-2021

Een welgemeende goedemorgen op deze zondagmorgen 4 juli 2021, een update vanuit het team VelzArt in Waardenburg. Na een succesvolle nacht van veel herstelde servers van onze klanten zijn onze buitendienst mensen inmiddels weer op pad om terug te plaatsen én de volgende lichting servers weer op te halen. Positieve noot in deze: bij alle servers die tot nu toe zijn behandeld is nagenoeg probleemloos de back-up teruggelezen en blijken ook bij terugplaatsing weinig tot geen issues. Het contact met de klanten voor het proces halen en terugplaatsen loopt volop via onze accountmanagers met ook daarbij de boodschap: wij zullen in contact treden.

De berichtgeving vanuit onze leverancier is vooralsnog summier en niet hetgeen wij graag hadden willen horen. Feitelijk gezien gaat dit voor werkstations betekenen dat ook daar een volledige herinstallatie plaats moeten gaan vinden. De impact hiervan is uiteraard ook groot. De bereidwilligheid van onze klanten om zelf de handen uit de mouwen te steken is groot. Op dit moment zijn we bezig met één van onze klanten om de zelfwerk procedure uit te werken en te testen. In de update van 14.00 uur proberen wij een ieder hierin van de juiste informatie te voorzien.

Voor de duidelijkheid: een complete herinstallatie betekent in deze dat de lokale data van het computersysteem verloren zal gaan én daarmee ook software anders dan Windows. Onze eerste doelstelling is om zoveel mogelijk systemen weer te voorzien van een schone installatie inclusief onze beheersoftware ENOA. LET OP: dit is NIET de ENOA software vanuit Kaseya. Zoals aangeven in eerdere berichten maakte we inmiddels slechts voor specifieke doeleinde gebruik van de Kaseya software. De huidige ENOA software is van een compleet andere leverancier.

Deze zondag gaan we gebruiken om zoveel als mogelijk servers te herstellen en terug te plaatsen. De zelfwerk procedure zal worden opgesteld voor werkstations en uiteraard zullen we ook zelf starten met het proces voor het compleet inregelen van werkstations voor onze klanten.
De eerlijkheid gebied ons te zeggen: wij gaan een aantal klanten vandaag relatief blij kunnen maken, we gaan ook mensen moet teleurstellen. We hopen op een ieders begrip en geduld, ook vandaag en de komende dagen.

Om deze berichtgeving positief af te sluiten: we hebben gisteren vanuit diverse collega bedrijven de helpende hand toegereikt gekregen. In deze voor ons ook emotionele tijd een zeer prachtig gebaar. Het heeft ons oprecht verrast en geeft ook hier een fantastische moraal. Dank hiervoor! Deze middag gaan we intern in overleg om ook deze mogelijkheden te beoordelen en in te passen. Een fijne zondag en wij laten ons omstreeks 14.00 uur weer horen.

Update: 18:45 uur – 03-07-2021 (Servers)

Beste klant,

Inmiddels hebben we diverse updates verstuurd via e-mail, WhatsApp of telefonisch contact. In deze willen we ons richten specifiek op onze klanten met een serveroplossing op locatie of via ons CloudConnect platform.

De afgelopen 24 uur hebben we koortsachtig geprobeerd om prioriteiten te stellen, onze mensen op een zo effectieve manier in te zetten en keuzes te maken. Vele van onze klanten hebben via o.a. onze accountmanagers geprobeerd een status update op te halen via eerder genoemde kanalen. Begrijpelijk uiteraard en volledig terecht. We gaan qua directe communicatie ons voor nu even beperken tot e-mail verkeer, in ieder geval tot aan morgenochtend. De ‘communicatieve ploeg’ gaat nu naar huis om ook even tot rust te komen, om vannacht op plekken bij te springen maar in ieder geval om morgenochtend verder te gaan met communiceren. Alle servers die we deze nacht kunnen behandelen zijn in huis. De planning is rond voor vannacht en morgen. Vanaf morgenvroeg zullen we ook weer in contact treden met servers die we komen terug leveren en/of servers die we komen halen voor herstel werkzaamheden.

Met betrekking tot de werkplekken binnen de kantooromgeving krijgen we ook de vraag of klanten op dit moment zelf iets kunnen doen ter controle of ter reparatie. Op dit moment is hierop het duidelijk antwoord dat we hierin nog een opties hebben. Laat werkplekken uit staan en wij komen ook hierover op een later moment met mogelijk oplossingen.

We begrijpen een ieders situatie en de uitdrukkelijke wens om maandag weer operationeel te zijn, qua server en werkplekken. We gaan niet aan al deze wensen kunnen voldoen, helaas moeten we op dit moment zo reëel zijn. Nogmaals, sommige van ons gaan nu de batterij op laden maar qua techniek en dus herstel blijft alles doorlopen, in een maximaal mogelijk tempo.

De update van 22.00 uur komt met deze berichtgeving te vervallen. Wij zullen morgenochtend in de richting van 11.00 uur wederom ons laten horen via de mail / online kanalen. Uiteraard zullen we direct schakelen met klanten daar waar nodig en van toepassing. Rest ons voor nu om nogmaals te bedanken voor een ieders begrip en geduld. We zullen morgen zo veel als mogelijk ‘persoonlijke’ updates verzorgen. Ondanks alles een fijne avond toegewenst.

Update: 17:00 uur – 03-07-2021

Algemene update: onder het mom beter één bericht dan geen bericht een korte update vanuit team VelzArt. Inmiddels is ons pand nog verder omgedoopt tot een gecontroleerd crisiscentrum waarop zeer diverse plekken in ons pand de herstelwerkzaamheden plaatsvinden. In samenwerking met onze partner & klant Voet Verhuur uit Culemborg zijn alle stroompunten gecontroleerd om zo extra installaties op te kunnen zetten. Onze mensen rijden gecoördineerd door onze Barbara door het land om servers op te halen en na herstel / installatie ook weer terug te plaatsen.

Bovenstaande introductie doet waarschijnlijk al vermoeden dat we over de verdere herstel van computersystemen nog vrij weinig kunnen melden. De constateringen die we in vorige berichten hebben gemeld blijken nog steeds juist. De adviezen die eerder zijn gemeld blijven ook van kracht, laat computersystemen uit staan, of zet ze uit indien dit nog niet heeft plaats gevonden. Vanuit onze eigen techniek maar ook vanuit onze leverancier zijn er nog geen oplossingen geboden die we nu kunnen voorstellen. Gelukkig hebben we ook een behoorlijk aantal klanten waar weinig tot niets gebeurd is wat uiteraard voor ons ook fijn is om de druk ietwat te verlagen.

We doen onze uiterste best. Wilt u uw situatie kenbaar maken aan ons, geef dan zit zoveel als mogelijk door via https://velzart.nl/update. Onze mensen zullen ook deze nacht weer aan de slag zijn om alle herstelwerkzaamheden verder vorm te geven. Rond de klok van 22.00 uur zullen wij wederom een update uitzenden met hopelijk meer nieuws / bijzonderheden.

Update: 13:12 uur – 03-07-2021

Deze update is gericht op werkstations. Uit al onze contacten lijken wij op te kunnen maken dat systemen, die gisteren (02-07-2021) tussen 18.00 uur en 20:00 uur hebben aangestaan, zijn geïnfecteerd. Systemen die in die tijd uit hebben gestaan (of in slaapstand) en dus niet of later dan 20:00 uur zijn aangegaan niet zijn besmet. De kanttekening daarbij: tenzij er in het netwerk een besmette PC aanwezig is/was. De besmetting van PC naar PC lijkt vooralsnog ook niet te gebeuren maar wij durven dit nog niet met 100% zekerheid te zeggen.

Besmette systemen komen tot nu toe voor in verschillende varianten. Sommige systemen zijn volledig ontoegankelijk, met andere systemen kan nog gewerkt worden. Deze laatste systemen hebben wel de bekende bestanden (“C:\Windows\mpsvc.dll” en readme txt) maar hier is geen beperking op het werken in bijvoorbeeld de browser. Vooralsnog blijft het advies, zet het systeem uit en wacht op nadere berichtgeving vanuit ons (VelzArt).

De vraag die we uiteraard veel krijgen: wat moet er gaan gebeuren met geïnfecteerde computers? Helaas gaan wij voorlopig nog uit van volledige herinstallatie echter lopen hier de onderzoeken nog voor. Gezien de impact van deze beslissing zoeken we hier naarstig naar oplossingen.

Daar waar slecht nieuws is kunnen we ook goed nieuws melden. De impact van de ransomware aanval lijkt zich te beperken tot lokale data. Van data die gesynchroniseerd staat richting OneDrive en/of SharePoint, ofwel de Microsoft Cloud, hebben wij nog geen probleem gevallen geconstateerd. De security layers van Microsoft hebben hierin goed hun werk gedaan.

Controle Microsoft Cloud
Wilt u zeker weten of uw Cloud bestanden wel of niet goed zijn, log dan in bij Microsoft via https://office.com.
Meer info over inloggen op Office.com kijk hier. LET OP: doet dit op een systeem wat niet geïnfecteerd is. Via de buttons richting SharePoint en/of OneDrive komt u rechtstreeks bij de bestanden. Zijn de bestanden daar in de browser te openen dan lijkt ook uw omgeving schoon van besmetting in de Cloud.

De overige update is dat de contacten met onze leverancier in volle gang zijn. Onze mensen hebben inmiddels een groot gedeelte servers opgehaald en een aantal servers zijn al weer onderweg terug om weer operationeel gemaakt te worden. Zoals eerder aangegeven, de impact is enorm. We verblijven in de gelukkige omstandigheid dat onze klanten zeer goed met ons meedenken wat ook weer moraal geeft aan onze eigen mensen. Ook deze klus gaan we klaren, bedankt ook voor een ieders geduld en begrip.

Voor vragen over de controle van uw eigen systemen verwijzen we graag terug naar de eerdere berichtgeving.
De volgende update zal tussen 16.00 en 17.00 uur zijn vandaag.

Update: 10:12 uur – 03-07-2021

Een bericht waarvan we gehoopt hadden nooit te hoeven versturen: een wereldwijde ransomware aanval zorgt sinds gisterenavond voor grote problemen bij onze klanten. We werken rond de klok aan oplossingen voor onze klanten. De nachtshift is om 08.00 uur deze ochtend afgelost door de dagshift, voor de beeldvorming. Een korte update vanuit VelzArt omtrent dit onderwerp.

Sinds 2010 maken wij gebruik van software van de organisatie Kaseya voor het beheren en onderhouden van computersystemen bij onze klanten. Ondanks de transitie die we zeer recent hebben gemaakt richting een nieuwe software oplossing stond de Kaseya software nog op veel van de systemen bij onze klanten voor specifieke beheerdoeleinden. De ransomware aanval is zoals gezegd wereldwijd, zie ook de volgende berichtgeving vanuit verschillende bronnen.

Berichtgeving Nu.nl
Berichtgeving NCSN

In samenwerking met onze partner en met vereende krachten binnen onze organisatie werken we aan oplossingen voor onze klanten. We hebben onze klanten sinds gisterenavond via telefoon, e-mail en nieuwsbrieven geïnformeerd over de voortgang van alle gaande zaken. Mocht u klant zijn van VelzArt en de berichtingeving helaas niet hebben ontvangen, meld u dan aan voor de berichtgeving via https://velzart.nl/update. We zullen dan zo spoedig als mogelijk u updaten. We proberen zoveel als mogelijk ook telefonisch zaken af te handelen echter gezien de impact van de aanval is dit in veel gevallen lastig.

Het belangrijkste advies is voor systemen die door ons beheerd worden:

- Laat computersystemen uit staan!
- Ze computersystemen uit die nog aan staan.
- Wacht op nadere berichtgeving.
- Meld je aan, indien eerdere berichtingeving gemist via velzart.nl/update.

Hou onze website en/of socials in de gaten voor volgende updates.
De volgende update wordt verwacht vandaag 03-07-2021 tussen 13.00 en 14.00 uur.

Wellicht ook interessant

ALS Sunrise Walk

Wij helpen mee in de strijd tegen ALS en zullen in de nacht van vrijdag op zaterdag 12 februari de zonsopgang tegemoet lopen.

Goede voornemens

Januari is dé maand om met een frisse blik vooruit te kijken en doelen te stellen voor jouw bedrijf, ook op IT-vlak!

Microsoft Teams webinar

Wat is microsoft teams, en hoe kan ik op een goede manier online samenwerken? Neem deel aan onze webinar en kom alles te weten over Microsoft Teams.

Concept & realisatie door Toon