V&K-CERT

1. Over dit document

Dit document beschrijft de dienstverlening van V&K-CERT: de organisatie, de services en policies.

CERT staat voor Computer Emergency Response Team en is een team binnen Van der Veen & Kromhout dat zich richt op de beveiliging van IT systemen – zowel de interne systemen van V&K als de systemen die via V&K-online voor klanten van V&K toegankelijk zijn.

Een andere veel gebruikte term is CSIRT, of Computer Security Incident Response Team. Beide termen betekenen hetzelfde.

Gezien het steeds verdere automatisering van de bedrijfsprocessen en daarmee de toenemende afhankelijkheid van IT met de daarbij onderkende potentiële vergaande risico's is besloten om een CERT team in te richten. Dit team is zowel gericht is op de eigen V&K organisatie als op klanten, met zowel een pro-actieve als reactieve dienstverlening.

De structuur van dit document is volgens RFC 2350.

1.1. Laatste update

Dit is versie 2.0, gepubliceerd op 22 augustus 2018.

1.2. Distributie van updates

De lezer dient zelf zeker te stellen dat dit de laatste versie van het document is.

1.3. Locatie van het document

De laatste versie van dit document kan gevonden worden op https://www.kromhout.com en op het V&K intranet in het kennissysteem van TOPdesk onder vaktechnische informatie → CERT.

2. Contact informatie

2.1. Teamnaam

"V&K-CERT": het Computer Emergency Response Team van V&K.

2.2. Postadres

Van der Veen & Kromhout
T.a.v.: V&K-CERT
Postbus 55
8400 AB Gorredijk
Nederland

2.3. Tijdszone

V&K-CERT hanteert Central European Time (CET), inclusief Daylight Saving Time (DST).
Als zodanig dus GMT+0100 in de winter en GMT+0200 in de zomer.

2.4. Telefoonnummers
Medewerkerkers V&K: alleen per e-mail bereikbaar
Klanten V&K: alleen per e-mail bereikbaar

2.5. Fax nummers
Medewerkers V&K: alleen per e-mail bereikbaar
Klanten V&K: alleen per e-mail bereikbaar

2.6. Andere communicatiemiddelen
Geen.

2.7. E-mail adres
cert@kromhout.com

2.8. Public keys en andere encryptie informatie
V&K-CERT gebruikt geen PGP voor het signeren van alle elektronische communicatie.
.

2.9. Website
V&K-CERT onderhoudt op dit moment (nog) geen eigen website.

2.10. Teamleden
De lijst met teamleden is niet publiek, doch uitsluitend intern beschikbaar op het V&K intranet in het kennissysteem van TOPdesk onder vaktechnische informatie → CERT.

3. Charter

3.1. Missie statement
De missie van V&K-CERT is het pro-actief en reactief ondersteunen van klanten en medewerkers van V&K in het verbeteren en op hoog niveau houden van de beveiliging van de IT dienstverlening.

3.2. Doelen
De doelen van V&K-CERT zijn:

- Zijn van een Single trusted point voor Internet security issues
- Creëren van awareness voor Internet security
- Geven van Internet security aanbevelingen
- Ondersteunen bij het oplossen van Internet security incidenten
- Actief opsporen en verwijderen van virusverspreiders, open relays en spammers
- De behandeling van meldingen van (potentiële) datalekken op basis van de AVG (Algemene Verordening Gegevensbescherming) en aanverwante wetgeving

3.3. Doelgroepen (constituencies)
V&K-CERT kent twee doelgroepen:

1. Klanten van V&K, waaronder gebruikers van V&K-online
2. Medewerkers van V&K.

3.4. Sponsors
V&K-CERT is onderdeel van de activiteiten van Van der Veen & Kromhout.

3.5. Bevoegdheden
V&K-CERT heeft in beginsel slechts een adviserende en motiverende functie en als zodanig dus geen bevoegdheden, tenzij zich een situatie voordoet (bijvoorbeeld bij een ernstig security incident) waarbij het nemen van maatregelen, in wat voor vorm dan ook, onmiddellijk noodzakelijk is.
Daarnaast beoordeelt V&K-CERT in hoeverre geconstateerde datalekken bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) dienen te worden gemeld en voert indien noodzakelijk deze meldingen uit.

4. Policies
Alle policies die gehanteerd worden zijn afgeleid van het V&K automatiseringsbeleid. Voor het gebruik van het V&K-online platform door klanten (doelgroep 1) is hiervan een vertaling gemaakt in de vorm van de V&K-online Algemene Voorwaarden, terwijl ten aanzien van de AVG (Algemene Verordening Gegevens-bescherming) een vertaling gemaakt is in de vorm van de V&K Privacyvoorwaarden. De laatste versies van

deze documenten zijn beschikbaar op de website https://www.kromhout.com

4.1. Incident typen en support niveau

V&K-CERT behandelt in principe alle typen security incidenten die plaatsvinden, of dreigen plaats te vinden, binnen de doelgroepen, op basis van zowel slachtoffer als dader. V&K-CERT probeert bovendien te reageren op verzoeken uit de doelgroepen.

Het support niveau dat wordt geleverd door V&K-CERT varieert, afhankelijk van het type en urgentie van een incident of issue, de grootte van de getroffen groep gebruikers of systemen en de beschikbare resources op dat moment, alhoewel er altijd binnen 1 werkdag een inhoudelijke response zal worden gegeven (buiten een eventuele autoreply). Toewijzen van resources gebeurt aan de hand van de volgende basale prioriteitsstelling (in afnemende prioriteit):

- Aanvallen op of vanuit doelgroep 1.
- Aanvallen op of vanuit doelgroep 2.
- Abuse, zoals probes, spam en virussen.

Alle andere typen incidenten worden intern geprioriseerd afhankelijk van hun ogenschijnlijke impact en schaal en kunnen al dan niet behandeld worden. Incidenten die geen betrekking op de 2 doelgroepen worden niet in behandeling genomen.

V&K-CERT bevordert het inschakelen van bevoegd security personeel van de betrokken organisatie in een zo vroeg mogelijk stadium.

Alhoewel V&K-CERT beseft dat er een grote variëteit is in het niveau van expertise bij de beheerders uit de constituencies, en hoewel V&K-CERT zal proberen om informatie te geven en assistentie te verlenen op een niveau dat geschikt is voor de betreffende beheerder, verleent V&K-CERT geen training on-the-fly en doet ook geen beheer voor de klant. In voorkomende gevallen zal V&K-CERT, waar mogelijk, verwijzingen geven naar de informatie die nodig is om de aangegeven maatregelen te implementeren.

V&K-CERT maakt zich hard om haar doelgroepen pro-actief op de hoogte te brengen van mogelijke vulnerabilities (m.a.w. voordat ze misbruikt worden) en zal bovendien de buitenwereld trachten te informeren over zulke vulnerabilities.

4.2. Samenwerking en interactie

V&K-CERT onderhoudt voor zover noodzakelijk relaties met wetgevende instanties.

Bovendien werkt V&K-CERT zo nodig nauw samen met andere CERT/CSIRT teams wereldwijd.

Er zijn wettelijke restricties aan de informatiegang van V&K-CERT (bijvoorbeeld de AVG, Algemene Verordening Gegevensbescherming), alsmede beleid vanuit V&K, eventueel aangevuld met policies van de doelgroepen, die (in deze volgorde) alle zoveel mogelijk gehonoreerd worden. Alle mogelijke maatregelen zullen bovendien genomen worden om de identiteit van individuele personen en systemen of groepen personen en organisaties te beschermen.

4.3. Communicatie en authenticatie

Gezien de typen informatie waar V&K-CERT mee te maken heeft wordt telefoonverkeer als voldoende veilig gesteld, ook zonder scrambling. Dit geldt voorlopig ook voor ongeëncrypte e-mail voor het uitwisselen van informatie die niet zeer vertrouwelijk is

Wanneer het noodzakelijk is een basis van vertrouwen op te bouwen, bijvoorbeeld voor het doorgeven van informatie aan V&K-CERT, of het verstrekken van vertrouwelijke informatie door V&K-CERT, zal de identiteit van de andere partij vastgesteld moeten worden met enige mate van zekerheid. De garantie van bekende en vertrouwde personen binnen de betrokken partij zal voldoende zijn om de identiteit van iemand vast te stellen. In alle andere gevallen zullen andere methodes worden gebruikt, zoals het gebruik van WHOIS gegevens of andere registratie gegevens op het Internet, etc, gecombineerd met call-back voor telefoon en mail-back voor e-mail om fraude uit te sluiten. Van binnengekomen e-mail waarvan de gegevens vertrouwd dienen te worden, zal de herkomst met de afzender persoonlijk worden geverifieerd.

5. Services

5.1. Incident response

V&K-CERT assisteert in de technische en organisatorische aspecten van security gerelateerde incidenten. Zie ook paragraaf 4.1 voor het support niveau.

Incident registratie
Alle incidenten worden geregistreerd. Na controle of er inderdaad een incident plaatsvindt of heeft plaatsgevonden, wordt het incident op basis van impact en urgentie verder uitgezet binnen de organisatie.

- Incident coördinatie

  Gedurende de looptijd van het incident worden diverse stappen ondernomen, zoals:

  - Bepalen van de oorzaak, of gebruikte vulnerability.
  - Faciliteren in contacten met andere organisaties die betrokken zijn.
  - Eventueel faciliteren in contacten met wetgevende instanties.
  - Eventueel waarschuwen van andere CERT/CSIRT teams.
  - Eventueel inlichten van de buitenwereld (andere klanten).
  - Eventuele escalatie en/of crisismanagement.

- Incident oplossing

  Het daadwerkelijk oplossen van een incident wordt in beginsel niet door V&K-CERT gedaan. Wel ondersteunt V&K-CERT in diverse vervolgstappen:

  o Verder onderzoek (forensics) naar achtergelaten sporen of binaries (artifacts).
  o Evaluatie en rapportage.
  o Eventuele juridische of disciplinaire vervolgacties.

Daarnaast zet V&K-CERT zich actief in om, binnen de doelgroepen, virusverspreiders, open relays en spammers op te sporen en te verwijderen.

5.2. Pro-actieve services

Om incidenten zoveel mogelijk te voorkomen biedt V&K-CERT diverse pro-actieve diensten:

- Uitbrengen van advisories

  Over beveiligingslekken worden doorgaans advisories uitgebracht door leveranciers en/of security teams, waarin vermeld staat wat precies het probleem is en welke oplossing er is gevonden - veelal in de vorm van patches van de leveranciers. Deze zijn doorgaans vrij beschikbaar op de websites van de leveranciers. Indien noodzakelijk worden deze advisories onder de doelgroepen verspreid, bij voorkeur vertaald in normaal Nederlands en begrijpelijk voor niet-technici.

- Technology Watch

  Hieronder wordt verstaan het volgen van mailinglists, security websites en andere nieuwsvoorzieningen over nieuwe technische ontwikkelingen en trends uit "de hackerswereld" die direct of in de toekomst een gevaar kunnen vormen. Ook nieuwe beveiligingstools en methodieken worden op deze manier gevolgd, die kunnen resulteren in advisories, richtlijnen of aanbevelingen.

5.3. Kwaliteitsmanagement services

- Creëren van awareness

  Hoe meer men zich bewust is van beveiligingsrisico's, hoe kleiner de kans op incidenten. Door mensen actief te blijven informeren hopen we deze bewustwording te creëren.

- Onderhouden van security FAQs

  Veel vragen worden meer dan eens gesteld (Frequently Asked Questions). Door deze vragen, met de daarbij horende antwoorden, publiekelijk beschikbaar te stellen, kunnen mensen sneller en beter worden geholpen.

- Kennispool op het gebied van security

  Alle binnengekomen informatie wordt centraal bewaard, waardoor historische gegevens, incidenten en advisories op een later tijdstip geraadpleegd kunnen worden.

- Business Contingency Planning

  De dienstverlening moet te allen tijde door kunnen draaien - in geval van grote incidenten moet uitgeweken kunnen worden naar een andere locatie, om aldaar de dienstverlening voort te zetten of in zeer korte tijd opnieuw op te bouwen. V&K-CERT adviseert over dit onderwerp.

- Crisismanagement

  Zeer zware incidenten kunnen vanuit een apart crisisteam worden gedirigeerd, waardoor de V&K-CERT organisatie ontlast wordt en zich volledig kan richten op het oplossen van het incident. Het crisisteam neemt ook alle contacten met de buitenwereld over, zoals communicatie met de pers.

6. Meldingsformulieren

Meldingsformulieren zijn (nog) niet beschikbaar.

7. Disclaimers

V&K-CERT kan de beschikbaarheid en juistheid van de in dit document voorkomende gegevens niet volledig garanderen. V&K-CERT aanvaardt geen enkele aansprakelijkheid voor schade ontstaan door afwezigheid of onjuistheid van de weergegeven gegevens, behalve indien deze schade te wijten is aan opzet of grove schuld.