Hack ROC Mondriaan

21 augustus 2021

MBO opleider regio Haaglanden

27 scholen

+/- 240 opleidingen

20.000 mbo-studenten

5.000 cursisten

> 2100 medewerkers

> 50 samenwerkingsverbanden

Hack ROC Mondriaan

21 augustus 2021

23 aug

Eerste schooldag

?

Omvang nog niet bekend

Kunnen we nog wel bij de roosters?

Hoe gaan we de studenten bereiken?

1e FASE

- Constatering hack
- Opstart crisismanagement
- Besluit IT

1e FASE

Constatering hack
- Verdachte bewegingen
- Beheerder naar locatie
- Servers ontkoppelt
- Contact SURFcert
- Inhuur NFIR

Opstart crisismanagement
- Start CMT
- Inlichten AP
- Alternatieve communicatie
- Inventarisatie applicaties
- Bepalen impact (onderzoek)

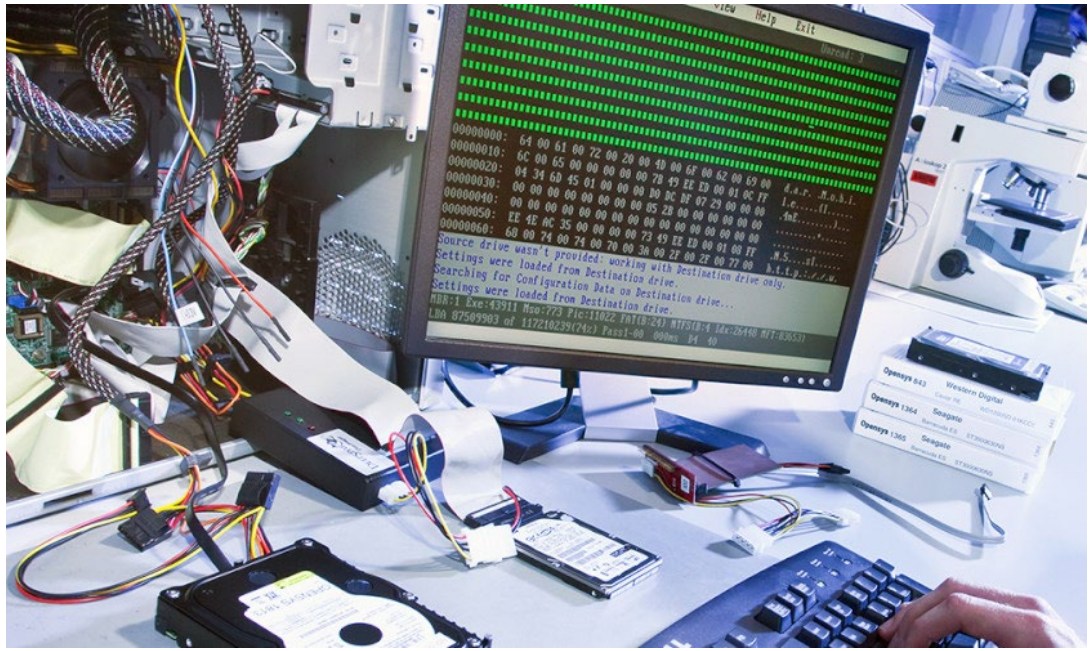
Besluit IT
- Uitzetten compleet IT-netwerk/omgeving
- Overleg met NFIR en SURFcert

De omgeving is dermate gecompromitteerd dat het hergebruiken van de bestaande systemen leidt tot een onaanvaardbaar beveiligingsrisico voor de toekomst.

Twee belangrijke uitgangspunten

het onderwijs gaat door
&
wij betalen niet

Nieuwe werkelijkheid



Nieuwe werkelijkheid

Nieuwe werkelijkheid

Magister

Nieuwe werkelijkheid

Nieuwe werkelijkheid

Nieuwe werkelijkheid

Nieuwe werkelijkheid

Kan ik klassenlijsten krijgen?

Kunnen jullie printers regelen?

Wanneer is er weer WiFI?

Hoe doen we het met de digitale examens?

Al mijn voorbereidingen waren opgeslagen, kan ik daarbij?

OCW wil graag in gesprek over de voortgang van het onderwijs

De pinautomaten doen het niet…

Zijn mijn gegevens wel veilig?

Een journalist heeft vragen gesteld

Hoe doen we registratie van aan- en afwezigheid?

Kunnen we onze crediteuren wel betalen?

De salarissen moeten bijna worden betaald. Gaat dat wel lukken?

Wij geven les mbv tekenappl. Wanneer werkt dat weer?

Leveranciers stellen veel vragen over de hack …..

Kan ik dit bestand wel gebruiken?

Wanneer doet het reserveringsysteem het weer?

Ik kan mijn privedevice toch wel gebruiken?

Een student heeft toch een computer aangezet…Is dat erg?

3 besturingslijnen

3 besturingslijnen

Forensisch IT onderzoek

Opbouw IT landschap

Korte termijn

3 besturingslijnen

- Heeft (veel) tijd nodig
- Zorgvuldigheid, volledigheid
  - Welke wijze ongeautoriseerde toegang heeft plaatsgevonden tot de omgeving(en).
  - Welke handelingen zijn uitgevoerd in het tijdsbestek waarin ongeautoriseerde toegang is verkregen
  - Welke systemen/data zijn geraakt
  - Wat is het eerste moment dat als veilig beschouwt kan worden

3 besturingslijnen

Forensisch IT onderzoek

Opbouw IT landschap

Korte termijn

- Veiligheid v snelheid
- Organisatie wil/moet verder
  - 1-2 jaar in een paar maanden
- Vernieuwing = ook leren
- Versneld keuzes maken
- Externe partijen
- Organisatie meenemen
- Authenticatiebeleid

3 besturingslijnen

- School open!
- Communicatie
- Ad hoc issues
  - Bestanden/ roosters/ zorgen
- Belangrijkste applicaties beschikbaar
  - HR2day, Magister, PortalPlus
- Laptops

Never waste a good crisis

Verbeteringen na hack

Verbeteringen na hack

- Aangescherpt authenticatiebeleid
- **Herinstallatie servers/ PC's etc**
- CIS-level 1
- **Netwerksegmentering**
- Endpoint security
- **CISO**
- Logging & monitoring
- **Awareness organisatie**
- Aanscherping devicebeleid

adviezen/aandachtspunten

Voorkomen

- Nooit 100%
- MFA =>
  ook voor studenten
- Endpointsecurity
- Hardening

[1] Hardening: proces waarbij overbodige functies en/of veiligheidsrisico's worden uitgeschakeld en verbindingen worden versleuteld. Dit om het mogelijke aanvallers zo moeilijk mogelijk te maken om toegang tot een systeem te verkrijgen.

adviezen/aandachtspunten

Voorkomen

- Nooit 100%
- MFA =>
  ook voor studenten
- Endpointsecurity
- Hardening

Schade beperken

- Netwerksegmentering (bescherm je kroonjuwelen)
- Data-beleid en handelen (= gedrag) (let op de kroonjuwelen)
  - Data-kwalificatie

[1] Hardening: proces waarbij overbodige functies en/of veiligheidsrisico's worden uitgeschakeld en verbindingen worden versleuteld. Dit om het mogelijke aanvallers zo moeilijk mogelijk te maken om toegang tot een systeem te verkrijgen.

adviezen/aandachtspunten

Voorkomen

- Nooit 100%
- MFA =>
  ook voor studenten
- Endpointsecurity
- Hardening

Schade beperken

- Netwerksegmentering (bescherm je kroonjuwelen)
- Data-beleid en handelen (= gedrag) (let op de kroonjuwelen)
  - Data-kwalificatie

Continue aandacht

- Organiseer ruimte voor een kritische blik/ waakhond (CIO/CISO)
- Onderwijs/business-belang & gebruikersgemak v securitybelang

[1] Hardening: proces waarbij overbodige functies en/of veiligheidsrisico's worden uitgeschakeld en verbindingen worden versleuteld. Dit om het mogelijke aanvallers zo moeilijk mogelijk te maken om toegang tot een systeem te verkrijgen.

adviezen/aandachtspunten

Voorkomen

- Nooit 100%
- MFA =>
  ook voor studenten
- Endpointsecurity
- Hardening

Schade beperken

- Netwerksegmentering (bescherm je kroonjuwelen)
- Data-beleid en handelen (= gedrag) (let op de kroonjuwelen)
  - Data-kwalificatie

Continue aandacht

- Organiseer ruimte voor een kritische blik/ waakhond (CIO/CISO)
- Onderwijs/business-belang & gebruikersgemak v securitybelang

Investeren in IT-security is geen keuze meer……

- Krachten (nog) meer bundelen?

[1] Hardening: proces waarbij overbodige functies en/of veiligheidsrisico's worden uitgeschakeld en verbindingen worden versleuteld. Dit om het mogelijke aanvallers zo moeilijk mogelijk te maken om toegang tot een systeem te verkrijgen.

Vragen??