VGR

VÄSTRA GÖTALANDSREGIONEN

Presentation av VGR

Ca 60.000 användare
1.6 miljoner medborgare
Vårdar ca 130.000 människor varje dag
Årlig budget på 50 miljarder

VÄSTRA GÖTALANDSREGIONEN

Presentation av VGR

18st sjukhus
Vårdcentraler
Tandvård
Psykmottagningar
Göteborgs Operan
Film i Väst
Västtrafik
Naturbruksgymnasium & folkhögskolor

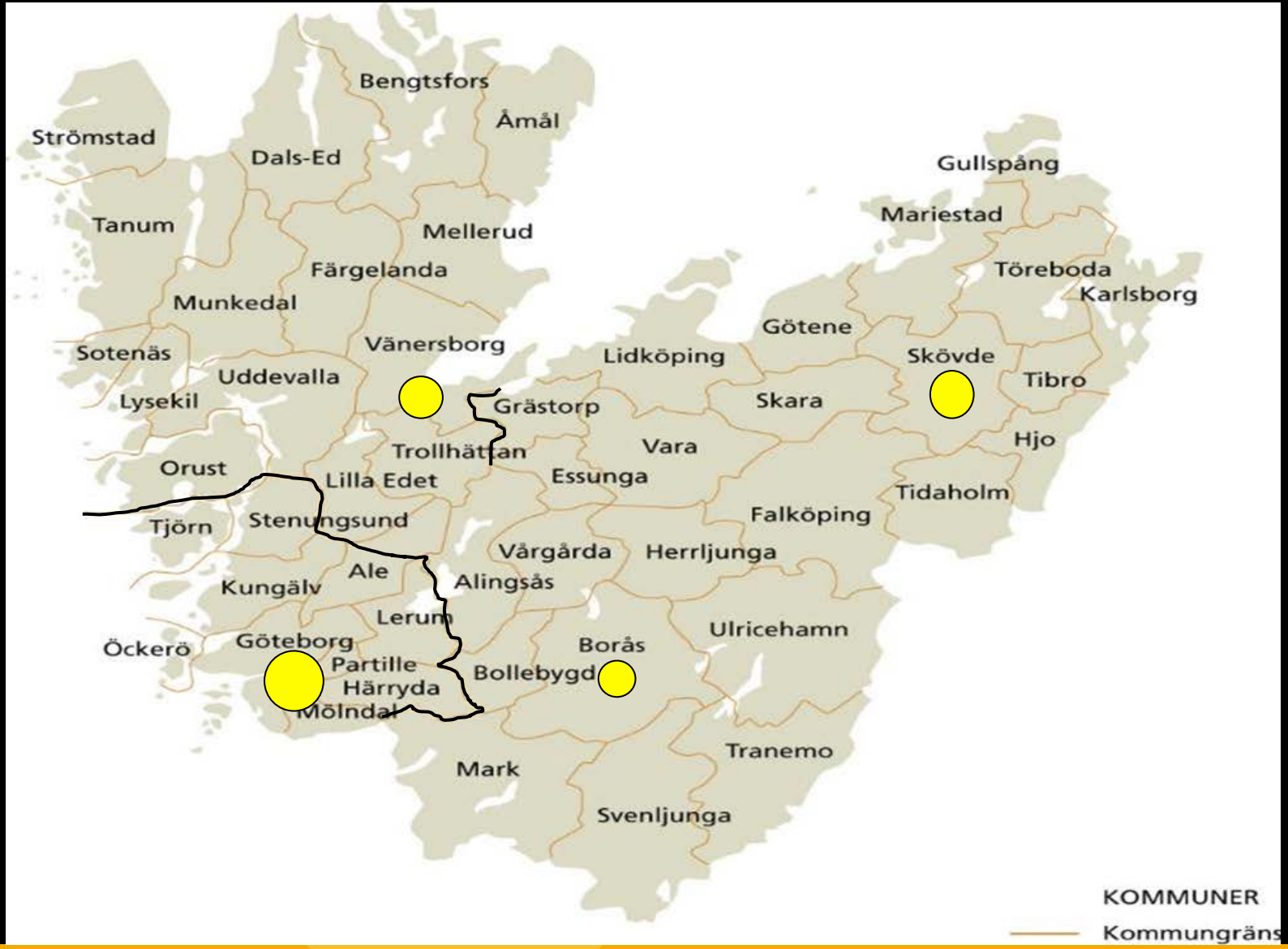
VGR finns på ca 500st unika adresser runt om i Västra Götalands regionen

Presentation av VGR IT

VGR IT har ca 700 anställda
Sitter under Regionstyrelsen
Hanterar ALL IT inom VGR
24/7 övervakning med beredskapskedjor
Ca 60000 pc, 180000 IOT
3-4000 servrar

VÄSTRA GÖTALANDSREGIONEN

VGR IT Kontor



VGR IT
Sektion IKT Säkerhet

VÄSTRA GÖTALANDSREGIONEN

Sektion Säkerhet - Team

Drift

Drift och förvaltning av säkerhetsverktyg och applikationer

SOC

Security Operation Center

Hantering av IT-Säkerhetsevent och incidenter

IAM

Drift och förvaltning av VGR AD och dess kringkomponenter

COLAB

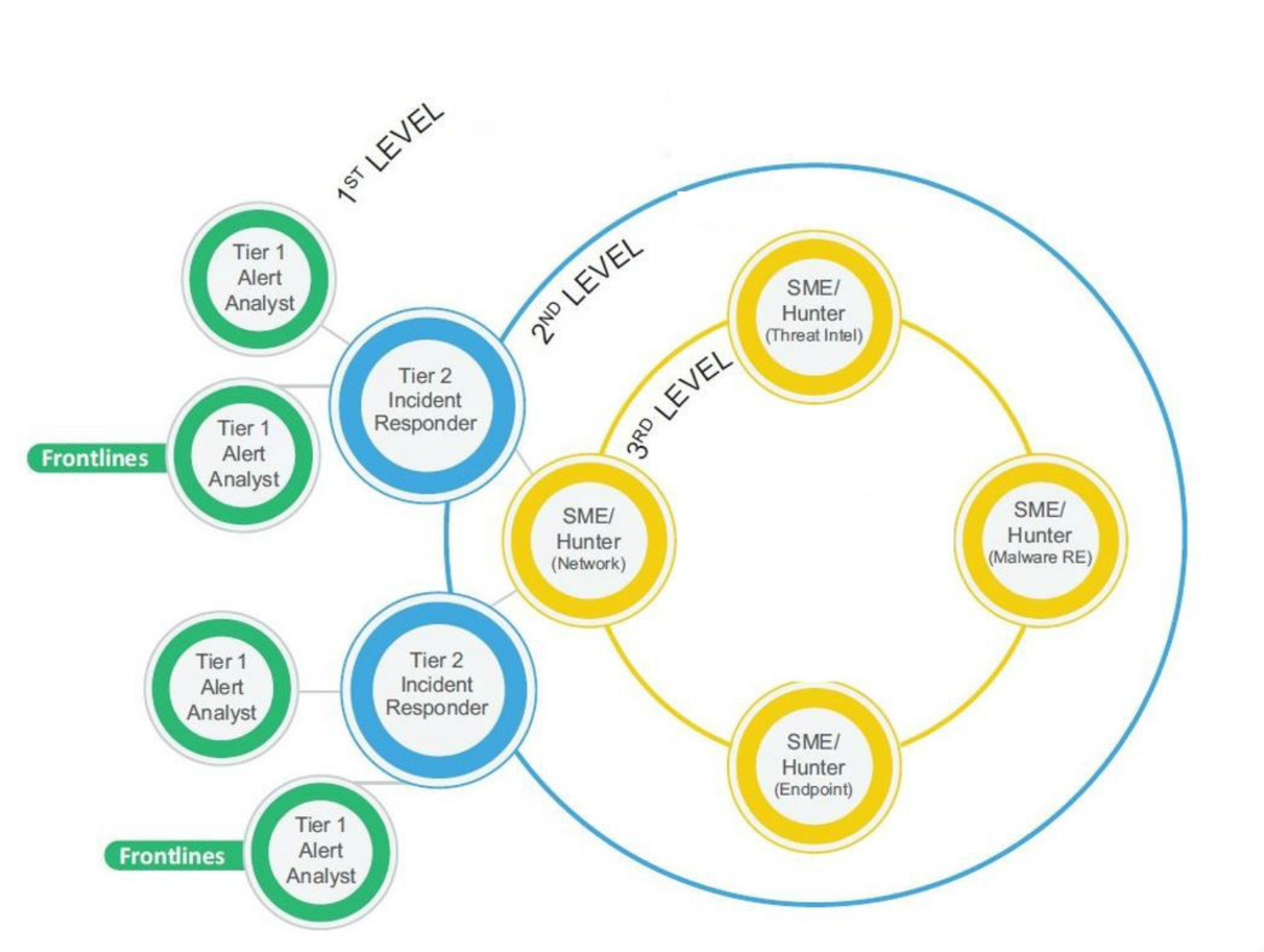
Drift och förvaltning av exchange/O365 samt sharepoint miljö

Säkerhet SOC

VÄSTRA GÖTALANDSREGIONEN

Uppdrag

- Prevention, Detection, Protection (Förebyggande, upptäcka, skydda)
- Active Defense (Aktivt försvar)
- Vulnerability Management (Sårbarhetshantering)
- Incident Response
    - » Investigation (Undersökning)
    - » Breach Notification (Intrångsnotifiering)
    - » Containment (Isolering)
    - » Eradication (Rensning)


1ST LEVEL
2ND LEVEL
3RD LEVEL
Frontlines
Frontlines
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Tier 2 Incident Responder
Tier 2 Incident Responder
SME/ Hunter (Threat Intel)
SME/ Hunter (Network)
SME/ Hunter (Malware RE)
SME/ Hunter (Endpoint)

Säkerhet SOC ansvarar för

- Omvärldsbevakning – Upptäcka zerodays-exploit
- Skapa ärende vid upptäckt av sårbarhet i plattform/system/applikation
- Hantering av IT-Säkerhetsincidenter/event
- Djupare undersökning/forensik

Säkerhetsverktyg & applikationer

- Brandväggar (HW/Virtuella)
- Web/DNSfilter
- Identitetshantering för Enheter (802.1x)
- Fjärraccess (VPN)
- SIEM
- IDS
- Klientskydd
- Användarbeteende analys

Vad är pågående just nu?

- Fortsatt utveckling av självservice
- Förändring av VPN-miljö
- Livcykelhantering av komponenter ex. firmware uppdatering m.m.
- Kontinuerligt pågående arbete med säkerhetshöjande åtgärder
- Slutförande av HTTPS Inspection på hela VGR’s produktionsnät

IT-Säkerhet

- Zero-trust
- Isolering
- Upptäckt av avvikande beteende
- Sårbarhetsskanning
- Kontinuerlig härdning av egen miljö

IT-Säkerhet – Vad är vi utsatta för?

- Phishing/Nätfiske
- Skadlig kod(virus/malware/ransomware/fileless malware)
- Cyberattack/DDOS-attack
- Rogue employee?

Utmaning

- VGR är Offentlig Sektor som styrs av politik, lagar och paragrafer, upphandlingar, offentlighetsprincip med mera.
- ”Molnet”
- Videomöten
- Pandemin
- Shadow IT
- Medicin teknisk utrustning – CE märkt produkt
- Våra användare

postnord

Du har lösta paket

Vi har fått ditt paket **CT429586028SE** på **2015/09/22**. Courier kunde inte leverera det här paketet till dig.

Få och skriva ut fraktsedel, och visa den på närmaste postkontor för att få det här paketet.

Få fraktsedel

Om paketet inte tas emot inom 20 arbetsdagar, kommer Postnord har rätt att kräva ersättning från dig - 60 kronor för varje dag för paketet lagring. Du kan hitta information om förfarandet och villkoren för paketet lagring i närmaste Postnord kontoret.

Detta är ett automatiskt meddelande. Klicka här för att avregistrera

PRESS ANY KEY!

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

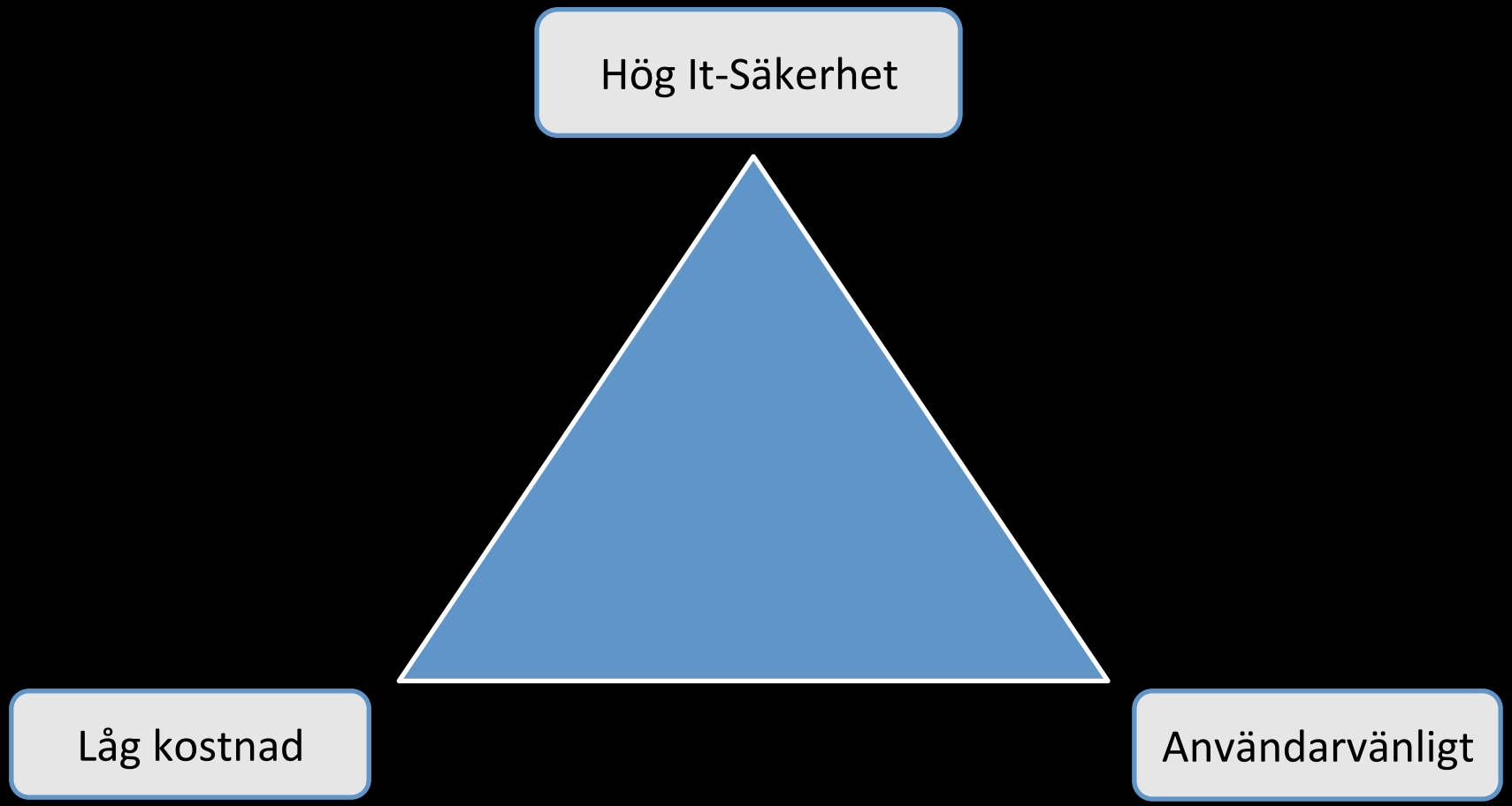
Let's Go Phishing!

VÄSTRA GÖTALANDSREGIONEN

Kostnad Virus/skadlig kod - Standardhantering

Tid per incident

- Ominstallation av dator + återläsning av backup = ca 2-3 timmar.
- Hantering av stoppa webb/nätfiske-länkar samt stopp av epostavsändare, rensning av mail både onprem och online = ca 30-120min
- Antal incidenter per månad = ca 30-50
- Totalt antal mantimmar ”kostar” ett skadlig kod-incident kund+VGR IT = ca 4-8 timmar.
- Totalt tid per år = 4800 timmar = 600 arbetsdagar


Hög It-Säkerhet
Låg kostnad
Användarvänligt

Jag har en leverantör som ska hålla en web-utbilning för sjukgymnaster via http://join.me/exorlive1 men den sidan verkar vara spärrad. Jag har skapat en ticket men inte fått svar ännu. Börjar bli lite bråttom

Kan du hjälpa mig?

Vad får du upp för sida när du inte kommer fram?

En sida som säger **Åtkomst till den begärda sidan har nekats.**

på grund av vad?

Innehåller någon typ av skadlig kod

precis

Men det är ju en vanlig sida att ha möten på

då ska vi absolut inte gå till den sidan

spelar ingen roll vi ska inte ha in skadlig kod till VGR

den är till för att skydda oss

Det står så här: Anledningen till att just denna webbsida blockeras är att den anses innehålla någon typ av skadlig kod eller annat innehåll som av säkerhetssystemet har klassats som riskfyllt eller innehåller annat oetiskt material.

japp stämmer

den som äger websidan måste rensa skadlig kod, sen öppnar vi upp automatiskt

Ok, då får vi hitta ett annat sätt.

VÄSTRA
GÖTALANDSREGIONEN