Myndigheten för samhällsskydd och beredskap

FAKTA

JUNI 2017

VERKSAMHETEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

Internetanslutna styrsystem i Sverige

En studie baserad på databaserna Censys och Shodan

I rapporten *Internetanslutna styrsystem i Sverige – En studie av Censys och Shodan* beskrivs en möjlig metod för att kunna svara på frågorna:

- **Vilka industriella informations- och styrsystem i Sverige är internetanslutna?**
- **Vilka komponenter inom svenska samhällskritiska verksamheter är internetanslutna?**

I detta till rapporten tillhörande faktablad ges en bakgrund till arbetet och tydliggörs några av studiens begränsningar.

I normalfallet finns det liten eller ingen anledning till att medvetet tillgängliggöra känsliga komponenter direkt på internet. I takt med att krav ställs på ökad tillgänglighet och utbyte av information mellan system, ökar dock också benägenheten att tillgängligöra systemkomponenter på distans. Resultatet från den här studien visar att potentiellt känsliga komponenter tillgängliggörs via publika, sökbara databaser även i Sverige. Alla organisationer som äger samhällsviktiga komponenter bör därför fundera över om sättet de internetansluts är tillräckligt säkert.

Studiens genomförande

Den studie som har genomförts har baserats på sökningar i publika databaser, d v s inga direkta frågor har ställts till komponenter. Aktiv scanning kan ge ett för frågeställningen mer uttömmande svar men kan skapa en onödig belastning på komponenterna.

Begränsningar

De öppna databaser som används har en stor begränsning inbyggd - de protokoll som täcks av Shodan och Censys är i huvudsak vinklade mot sådana som används i USA. Många av de i Sverige vanliga protokollen stöds inte alls vilket medför att det sannolikt finns styrsystemsutrustning som inte identifierades av studien.

Shodan och Censys

De publika databaser som användes i studien var i huvudsak Censys (https://www.censys.io/) och Shodan (https://www.shodan.io/). Båda dessa fungerar förenklat som sökmotorer likt Google (https://www.google.com/). Google indexerar främst webapplikationer såsom hemsidor. Censys och Shodan samlar med motsvarande metod aktivt in information från internetanslutna datorer men indexerar även data från andra serverapplikationer än web-applikationer. Exempel på utrustning som kan komma att indexeras är kameror, kopiatorer och enskilda komponenter i styrsystem (ex PLCs) om de är anslutna till internet.

Ingående sektorer

Organisationerna som ingick i studiens sökning kategoriserades som hemmahörande inom sektorerna elkraft, transport, sjukvård samt vatten och avlopp. Viktigt att notera är att vissa organisationer har IP-adresser som rör helt olika tjänster. Exempelvis kan en organisation både distribuera el och bredband och koppla IP-adresserna bakom dessa tjänster till samma namn vilket kan göra det omöjligt att urskilja om en komponent ägs av organisationen eller t ex en abonnent av organisationens bredbandstjänst. Detta påverkar resultatet avseende framför allt sektorn elkraft då både tjänsterna el och bredband i ovan exempel faller under elkraft.

Även urvalet av söktermer gällande såväl organisationer som teknologier påverkar resultatet. Det är rimligt att anta att endast en liten delmängd av alla relevanta söktermer identifierades av den genomförda studien.

Andra faktorer som begränsar och påverkar resultatet är exemplevis huruvida organisationerna använder NAT (Network Address Translation) för att exponera flera datorer mot internet via ett mindre antal IP-adresser samt vid vilken tidpunkt sökningen är gjord.

Resultat

Resultatet visar bland annat på stora skillnader mellan sektorerna. Särskilt sektorn elkraft sticker ut avseende antal indexerade komponenter. Anledningen till detta kan snarare tillskrivas de ovan beskrivna begränsningarna (gällande protokoll samt ingående tjänster inom sektorn) än på att det föreligger några faktiska skillnader mellan sektorerna.

Sökningen i studien kan upprepas och skapar på så sätt en möjlighet att följa utvecklingen över tid. Det är i huvudsak skillnader mellan sådana sökningar som är intressant snarare än de sammanställda resultaten i studien.

Vägledning

MSBs *"Vägledning till ökad säkerhet i industriella informations- och styrsystem"* innehåller 17 grundläggande rekommendationer för att öka säkerheten i industriella informations- och styrsystem.

MSBs vägledning går kostnadsfritt beställa eller ladda ner på:
www.msb.se/ics
eller kontakta oss på
scada@msb.se

Kontakta Myndigheten för samhällsskydd och beredskap

651 81 Karlstad

Publ.nr: MSB1111

Tfn: 0771-240 240
Fax: 010-240 56 25
registrator@msb.se
www.msb.se

Kontaktpersoner:
Anders Östgaard
anders.ostgaard@msb.se
Kristina Blomqvist
kristina.blomqvist@msb.se