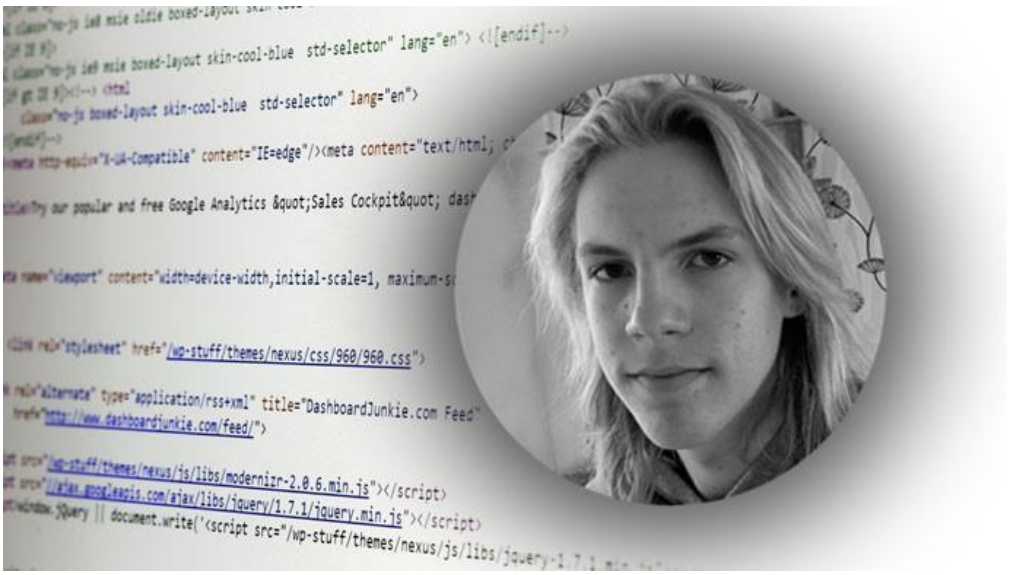
Av: Linus Särud **Skribent**

Linus Särud

Sluta gulla med hackaren

KRÖNIKA Det finns mer bakom domen mot 17-åringen än det som media har lyft fram i ljuset, säger Linus Särud, själv ung it-säkerhetsexpert och bug bounty-jägare.

Nyheten om 17-åringen Erik Sundqvist i Umeå som hackade kommunen och nu har blivit dömd för dataintrång har i senaste veckan cirkulerat i media. Media har valt sida och håller klart och tydligt på Sundqvist. Det har genomförts namninsamlingar mot kommunen och han ska ha erbjudits jobb inom it-säkerhetsbranschen.



Första gången jag läste rubrikerna blev jag inte bara sur utan rent ut sagt förbannad på Umeå kommun. Som it-säkerhetsintresserad händer det då och då att man drar iväg ett mejl till någon it-ansvarig för att tipsa om att någon säkerhetsbrist borde åtgärdas. Större internetföretag har ofta ett bug bounty-program och uppmanar därigenom folk att hitta sårbarheter och rapportera dessa för pengar. Även mindre företag som inte har sådana program brukar generellt bemöta folk som hör av sig på ett trevligt sätt.

Det finns dock undantag – det har till exempel hänt att jag har fått hot om polisanmälan som tack för tipset. Mitt medlidande och förståelse gentemot Sundqvist var alltså vid det här laget stort.

Jag begärde ut förundersökningsprotokollet och domen för mer objektiv syn på det hela och läste igenom den, och min tidigare starka sympati försvagades fort. Han har inte bara, som media valt att framställa det, blivit dömd för att rapportera några säkerhetsbrister. Hans dom lyder:

”[...] berett sig tillgång till uppgifter avsedda för automatiserad behandling genom att vid upprepade tillfällen med annans behörighet logga in på server och datorer tillhörande Umeå kommun och där ta del av information och ändra processoranvändningen.”

För att sammanfatta förundersökningsprotokollet som mer detaljerat beskriver händelsen ska han ha gjort följande:
• installerat en miner-mjukvara för Litecoin (kryptovaluta likt Bitcoin) på kommunens servrar (”ändra processoranvändningen”). *(Förtydligande 2015-03-28: Man har bevisat att Sundqvist har använt enorm datorkraft på kommunens servrar - det gör att det finns starka skäl att tro är för att han installerade en miner-mjukvara. Sundqvist själv säger att han inte minns huruvida så var fallet eller ej.)*
• tagit sig in i en dator som styr låssystem.
• fått tillgång till all data i Umeå kommun (inklusive Socialtjänstens journalsystem).
• klickat bort de larm som varnat för ökad belastning.
• varit inne på 30–40 av kommunens servrar.
• ha laddat ner hundratals lösenord. *(Förtydligande 2015-03-28: Sundqvist har med stor sannolikhet laddat ner hundratals lösenord – man kan se förfrågningarna, men man har inte lyckats bevisa att det faktiskt är lösenord han hämtat ut.)*

Det är dessutom inte första utan andra gången han åker dit för dataintrång.

Vad är då anledningen till Sundqvists handlande? Jag citerar förundersökningsprotokollet med förhör av Sundqvist:

”Han hade 3–4 samtal med ordföranden för nämnden, men efter det så rann det ut i sanden. Erik säger att han kände sig arg, frustrerad och inte mått bra för att ingen lyssnade på honom. Han bestämde sig därför för att visa kommunen och utförde därför dataintrånget.”

Sunt förnuft gäller även i it-sammanhang – ska man rapportera sårbarheter och vill bli bemött trevligt är det lämpligt att själv på trevligt sätt kontakta de drabbade. Jag har väldigt svårt att se att det är vad Sundqvist här skulle ha gjort, hans handlingar tyder snarare på egenintresse än vilja att hjälpa kommunen. Det här lär Sundqvist vara medveten om då han vidtagit flera åtgärder för att minimera risken att själv bli upptäckt, däribland spoofat sin mac-adress.

Det är tyvärr incidenter likt dessa som sabbar ryktet för oss som sysslar med it-säkerhet och framställer oss i dålig dager. Om än media har valt sida verkar majoriten av de jag pratat med inom branschen vara överens; Sundqvist har gjort fel och är inte så oskyldig som media vill framställa honom.

Visst, Umeå kommun borde ha agerat annorlunda och insett allvaret i ärendet. Deras ignorans legitimerar dock inte Sundqvists agerande. Man kan inte gå in genom en dörr och slå sönder allt innanför bara för att man redan påtalat att den var olåst.

Externa länkar

- Säkra e-posten - 7 åtgärder för skyddad kommunikation
- Våga ha åsikter – och våga ändra dem
- 50 000 attacker per dygn

Av: Lars Danielsson Reporter

Lars Danielsson

Så här undviker du falska säkerhetslarm

Om antalet säkerhetslarm blir väldigt högt ökar risken för att man missar de viktiga larmen. Här är tips om hur du kan undvika det.

Säkerhetslarm som visar sig inte vara några larm egentligen, så kallade falska positiva larm (false positives), är ett stort problem. Det är som i sagan med pojken och vargen. Om man ropar att vargen kommer en massa gånger när vargen inte kommer, så är det ingen som lyssnar till slut när vargen verkligen kommer.

Problemet med falska positiva larm vad gäller it-säkerhet är förstås att det blir informationskaos och risken finns att de larm som man verkligen skulle behöva bry sig om försvinner i mängden av larm.

Säkerhetsföretaget Fireeye har genomfört en undersökning bland it-säkerhetschefer. 37 procent av respondenterna uppger att de får fler än 10 000 larm per månad. 52 procent av dessa är falska positiva larm och 64 procent är redundanta. Det här innebär en stor arbetsbörda, eftersom man analyserar varje larm manuellt på 40 procent av företagen.

Läs också: Enormt bot-nätverk upptäckt – 15 000 servrar utvinner kryptovaluta i hemlighet

En undersökning gjord av Cisco, 2017 Security Capabilities Benchmark Study, visar att företag bara hinner analysera 56 procent av säkerhetslarmen varje dag. Hälften av dessa, alltså 28 procent av säkerhetslarmen, bedöms vara korrekta. Mindre än hälften av de korrekta larmen, 46 procent, alltså cirka 13 procent av alla larm, leder till någon åtgärd.

Enligt Ciscos undersökning får 44 procent av it-säkerhetscheferna ta del av fler än 5 000 säkerhetslarm varje dag.

Att det blir så många larm beror inte minst på att många företag använder flera övervakningsverktyg som ständigt analyserar nätverkstrafik och användares aktiviteter.