FOTO: ANDREAS BERONIUS

Full fart runt spelbrädet. *Kvällen före den officiella öppningen av 4 Sics, en internationell konferens om IT-säkerhet för styrsystem, samlades konferensdeltagarna runt spelborden. Målet var att driva ett kraftverk som utsätts för IT-attacker.*

Spelet som gör IT-säkerheten begriplig

Kips åskådliggör IT-säkerheten i produktionen så alla förstår hur viktig den är

Företaget vi jobbar åt har just köpt ett kraftverk och vår grupp har fått ansvaret för IT-säkerheten i produktionen. Ingen verkar ha skött detta tidigare, så vi vet inte hur det står till med cybersäkerheten eller vilka incidenter som kan ha inträffat. Nu är det vår uppgift att IT-säkerheten ska fungera så att anläggningen kan producera el med så små förluster som möjligt. Till vårt förfogande har vi en budget på 50 000 dollar och en begränsad tid som vi får lägga på uppgiften.

Det finns många saker vi skulle kunna göra för att öka IT-säkerheten. Några förslag är att utbilda personalen, dela upp nätet i skilda segment, inrätta en VPN-tunnel till PLC-leverantören eller kanske helt och hållet bryta kontakten med Internet. Allt har vi inte råd och tid med, så frågan är var vi ska börja

Sammanfattat

- Kips är en övning som ger insikt i IT-säkerhetens betydelse.
- Kips är utformat som ett spel och tar cirka två timmar att genomföra.
- Deltagarna delas in i lag med tre till fem deltagare.
- Spelet leds av en auktoriserad spelledare.
- Målet är att driften ska vara så lönsam som möjligt trots hackerattacker och andra IT-incidenter.

Sådant är utgångsläget. Nu kan spelet sätta igång.

Kips är en övning utformad som ett spel för att åskådliggöra IT-säkerhetens betydelse för en verksamhet. Deltagarna får i lag tävla med varandra om att få ett kraftverk att producera så mycket elektricitet som möjligt, trots att det under spelets gång utsätts för en mängd IT-attacker. Hur produktionen klarar av attackerna beror på vilka skyddsåtgärder gruppen vidtar och på hur den hanterar attackerna som dyker upp under spelets gång.

Ser effekterna av dålig säkerhet

– Det här är ett interaktivt sätt att lära sig vad IT-säkerheten betyder för verksamheten, vilka åtgärder man kan vidta och vilka konsekvenser brister i säkerheten kan leda till, förklarar Erik Johansson, en av grundarna till före-

FOTO: MY OLAUSSON

***Förutom spelplan** och aktivitetskort använder spelarna en Ipad där de får information om säkerhetsläget.*

”Alla händelser i spelet bygger på incidenter som verkligen har inträffat. Likaså är begränsningarna i tid och pengar realistiska.”

taget Omnisiens, som utbildar organisationer inom IT-säkerhet och dessutom är auktoriserad spelledare för Kips.

– Med Kips får deltagarna uppleva effekterna av dålig IT-säkerhet när en verksamhet blir attackerad. Man ser och upplever effekterna, samtidigt som man kan lära av andra, säger han.

Gäller att göra datanäten säkra

Första uppgiften är att försöka bygga kraftverkets olika datanät så säkra som möjligt med de resurser man har. När spelet fortsätter, blir det också en samarbetsövning i att klara incidentlägen.

– Det är mycket bättre att öva på hur man ska klara incidenterna innan det uppstår ett skarpt läge, menar Erik Johansson.

Vid första påseendet ser Kips ut som ett klassiskt sällskapsspel som Monopol eller Risk. Spelarna sitter samlade runt ett bräde som föreställer kraftverket som de ska driva, med dess viktigaste utrustning och dess datanät. Spelarna har också en mängd aktivitetskort de kan spela ut för att skydda sig mot attacker, kontrollera läget i anläggningen, få igång driften efter en incident, reparera sådant som gått sönder vid attackerna och förbättra datanäten. Varje kort är försett med en prislapp och med en tidsangivelse som markerar hur mycket tid som går åt för olika uppgifter.

– Kips är mer än bara en spännande aktivitet. Det kan fungera som en ögonöppnare för ledningsgruppen eller som en större aktivitet för att höja IT-säkerheten i en verksamhet, menar Erik Johansson.

Olika yrkesgrupper samverkar

Bäst resultat får man om varje grupp innehåller deltagare från flera yrkeskategorier som får diskutera sig fram till hur man bäst ska lösa uppgiften. Lagmedlemmarna kan vara anläggningsägare, företagsledare, IT-specialister lika väl som produktionstekniker eller tillhöra någon annan berörd yrkesgrupp.

Tre till fem personer är lagom. Är gruppen för stor, blir det svårt att enas om en handlingsplan.

– På det här viset får man igång ett samtal om dessa viktiga frågor, säger Erik Johansson.

– Deltagarna får en gemensam förståelse för utmaningar som anläggningen ställs inför, vilka beslut som behöver fattas och lär sig samverka över yrkesgränserna.

Det är med andra ord inte nödvändigt att vara IT-expert för att ha glädje av Kips. Tvärtom, genom aktivitetskorten får spelare som till vardags inte tänker på IT-säkerheten i produktionen

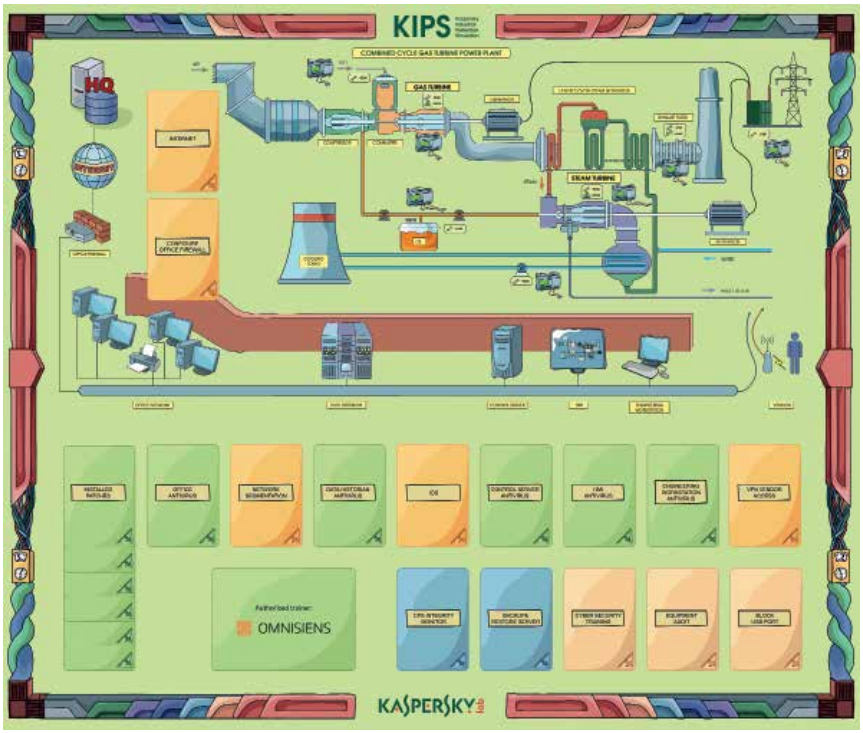

FOTO: ERIK JOHANSSON

***Kips finns i fem versioner.** En av dessa handlar om att ta hand om IT-säkerheten i ett kraftverk med gasturbin.*

lära sig vilka åtgärder man kan vidta. Och de ser vad som kan hända om man inte tar uppgiften på allvar, menar Erik Johansson. Inte minst visar spelet hur det kan påverka företagets ekonomi.

Vill nå ut bättre

Spelets namn Kips är en för kortning för Kaspersky Interactive Protections Simulation. Kaspersky, som är ett IT-säkerhetsföretag, utvecklade Kips som ett snabbt och intressant sätt att åskådliggöra vad som kan hända om inte IT-säkerheten fungerar, vilka motåtgärder man kan vidta och vilken betydelse arbetet har. Inte minst ville man nå företagsledningarna med detta budskap.

Diskussioner om IT-säkerhet riskerar alltför ofta att bli väldigt teoretiska för andra än dem som handgripligen arbetar med uppgiften. Det kan exempelvis handla om att IT-avdelningen överlämnar en 200-sidig rapport full med datatermer som är svåra att förstå för alla som inte är inne i tekniken. Även föredrag riskerar att bli mer eller mindre teoretiska.

– Kips får alla engagera sig praktiskt i uppgiften och ta konkret ställning till åtgärder och konsekvenser, säger Erik Johansson som påpekar hur mycket mer effektivt man minns sådant man upplevt jämfört med om man läst samma sak.

Bygger på verkliga händelser

– Visst är Kips tillrättalagt för att fungera i spelform. Men alla händelser bygger på incidenter som verkligen har inträffat. Likaså är begränsningarna i tid och pengar realistiska, påpekar Erik Johansson.

Vid spelets början får spelarna ett antal aktivitetskort, med åtgärder man kan vidta. Det kan vara allt från att byta lösenord till att utbilda personalen. Åtgärderna kostar tid och ibland också pengar, vilket begränsar de åtgärder man kan vidta med sin budget och den arbetstid man fått tilldelad. Under spelet utsätts laget för olika IT-relaterade händelser, incidenter och attacker, som kan påverka verksamheten och i värsta fall leda till produktionsstopp eller dyrbara reparationer. Exakt vilka konsekvenserna blir, beror på vilka skyddsåtgärder laget genomfört och hur man reagerar på de händelser som inträffar.

FOTO: DAG TOIJER

> **”Med Kips får deltagarna uppleva effekterna av dålig IT-säkerhet när en verksamhet blir attackerad.”**
>
> Erik Johansson, säkerhetsrådgivare på Omnisiens och auktoriserad spelledare.

Det är med andra ord avgörande vilka aktiviteter man vidtar, det vill säga vilka kort man spelar ut, både vid spelets inledning och hur man använder korten man har kvar när saker inträffar under spelets gång.

Två timmars speltid

Uppgiften är att hålla produktionen igång så bra som möjligt. Om allt fungerar friktionsfritt ger produktionen ett överskott på 200 000 dollar. Summan minskas av åtgärder man vidtar som kostar pengar och framförallt av skador och produktionsstopp som kan bli en följd av attackerna. Spelet är uppdelat i fem omgångar som tillsammans tar cirka två timmar.

– Det lag som tjänat mest pengar när spelet är slut står som segrare, förklarar Erik Johansson.

– Efter spelet gör vi en genomgång av vad som hänt och vilka åtgärder som kunde ha förbättrat resultatet. På så vis kan deltagarna dra lärdomar av spelet, avslutar han.

Dag Toijer

Spel för olika sorters verksamhet

BILD: ERIK JOHANSSON

Spelet Kips finns i fem versioner för olika typer av verksamheter. Två av spelen handlar om industriliknande produktion, dels ett kraftverk med gasturbin, dels ett vattenreningsverk. Utöver dessa finns spel för tre andra områden: bank, offentlig verksamhet med internettjänster samt ett handelsbolag.

Laget som klarar IT-attackerna bäst vinner

Kips spelas i fem omgångar med ökande tidspress för varje ny runda

Kips tar cirka två timmar att spela. Det spelas i fem omgångar och det lag som på slutet har tjänat mest pengar åt sitt företag står som segrare.

Varje omgång har fyra faser: information om läget, planering och aktiviteter, produktion och till sist rapportering. 200 000 dollar är värdet på den maximala produktionen under varje omgång. Från den summan drar man av kostnaderna för problem som uppstår på grund av IT-relaterade incidenter, exempelvis reparationer och produktionsstopp. Vidare tillkommer kostnaderna för de säkerhetsåtgärder man genomför.

Organiseras av en spelledare

Kips är inte ett spel man köper i affären och ger bort i julklapp, utan en organiserad övning som leds av en spelledare auktoriserad av företaget Kaspersky. I utrustningen ingår förutom spelbrädet och spelarnas aktivitetskort också en Ipad till varje grupp. Ipaden används för meddelanden från spelledningen under spelet. Den används också av spelarna för att mata in sina åtgärder.

Under första fasen av varje omgång får spelarna information om utgångsläget via sin Ipad. Dessa informerar om IT-incidenter som inträffat, säkerhetsluckor som upptäckts i operativsystem eller programvara och om problem i den egna verksamheten, exempelvis en PLC eller dator som uppför sig konstigt.

Väljer hur näten ska skyddas

Under fas två ska lagmedlemmarna komma överens om hur datanäten ska skyddas och som följd av det välja ett antal åtgärder. Varje lag utrustas med en bunt aktivitetskort som motsvarar de åtgärder man har att välja på, drygt 20 stycken. Korten beskriver aktiviteter som att undersöka vilken utrustning som är inkopplad på företagets nät (vilket precis som i verkligheten långt ifrån alltid stämmer överens med dokumentationen). Andra åtgärder kan vara att konfigurera brandväggar, installera antivirusprogram, ta bort skadlig programvara eller uppdatera, ”patcha”, programvara som har säkerhetsbrister. I kortbunten ingår också rena reparationer, exempelvis av en PLC eller till och med en skadad gasturbin.

Att välja alla korten är inte möjligt. Vart och ett av dem är försett med en prislapp och den tid som just den aktivteten tar. Gruppen tilldelas 50 000 dollar för hela spelet och 100 tidsenheter per spelomgång att använda.

FOTO: MY OLAUSSON

***Laget diskuterar** sig fram till vilka säkerhetsåtgärder som ska vidtas. Därefter placeras aktivitetskorten ut.*

> **”Att välja alla korten är inte möjligt. Vart och ett av dem är försett med en prislapp och den tid som arbetet tar.”**

Tidspressen ökar

Det gäller för gruppen att komma överens om vilka åtgärder man ska vidta med hänsyn till budgeten och den tid man disponerar. Den verkliga tidspressen ökar också genom att tiden för att komma överens om de första åtgärderna kortas för varje omgång. Den första spelomgången har deltagarna 10 minuter på sig, den sista omgången har man bara tre minuter.

I den tredje fasen startar driften. Men den får inte pågå problemfritt eftersom spelledaren hela tiden sätter igång olika IT-relaterade händelser som stör verksamheten. Detta får deltagarna meddelande om på gruppens Ipad. Alla grupper utsätts för samma attacker, men det innebär inte att alla drabbas på samma sätt. Effekterna beror på vilka skyddsaktiviteter som gruppen valde under fas två, och på hur spelarna löser problem som uppstår.

Efter en bestämd tid, avslutas produktionsfasen och utfallet summeras. När fem spelomgångar slutförts efter cirka två timmar koras vinnarlaget.

Dag Toijer