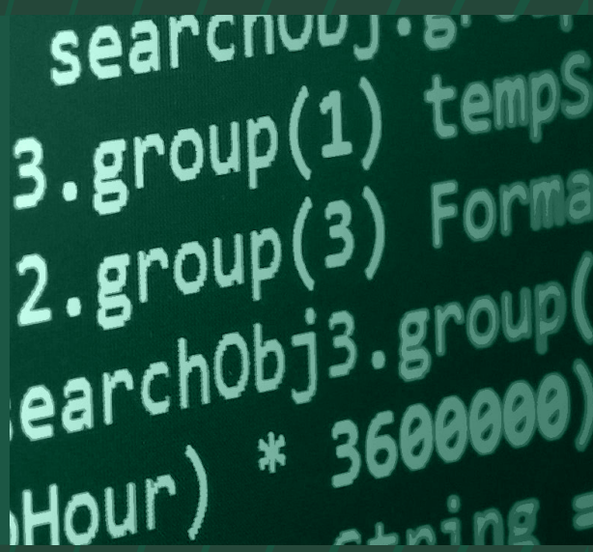
DELL Technologies

5 Rekommendationer för att klara en utpressningsvirusattack



1 Ha en omfattande incidentrespons-plan

- Fokusera på att minimera effekterna av en attack
- Öva, testa och uppdatera ofta
- Ha ett incidentresponsteam redo
- Fundera på cyberförsäkringar som en del av din övergripande tålighetsstrategi
- Inkludera planer för samarbete med brottsbekämpande myndigheter

2 Ha en tydlig kommunikations-strategi på plats

- Skapa kommunikationsmallar i förväg
- Säkerställ snabb och tydlig kommunikation inom organisationen
- Var redo att kommunicera externt, vid behov
- Följ gällande regelverk angående meddelanden

3 Säkerställ ett robust dataskydd

- Skydda kritiska data i ett isolerat, oföränderligt och avgränsat datavalv
- Prioritera återställning efter tjänst/ infrastruktur
- Öva på återställning
- Para ihop funktioner som renrum med ditt mål för återställningstid
- Säkerställ integriteten hos data som kan återställas

4 Förutsätt inte en omedelbar återgång till det normala

- Att betala en lösensumma bör vara en sista utväg
- Se till att lagar och regler efterlevs innan du betalar
- Ingen garanti för att hackaren skulle återlämna dina data även om en lösensumma betalas

5 Ha fokus på övning och utbildning

- Utför attacksimuleringar
- Övervaka och testa medarbetarnas säkerhetsrutiner
- Använd verktyg som nätfisketester och utbildning i e-postsäkerhet

Det är inte längre en fråga om ”om”, utan ”när”.

Företag måste planera som om en attack är oundviklig, trots deras bästa försvar. Dells ämnesexperter Jim Shook, Global Director of Cybersecurity and Compliance Practice, och Steven Granat, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, slog sig ned tillsammans med Brian White, Senior Consultant, Product Marketing, för Dell Data Protection, för att diskutera vad man ska göra när en katastrof inträffar.

> Du behöver ta in rätt personer, genomföra en övning och simulera åtgärder så att alla vet direkt vad de ska göra när en attack sker.”
>
> ***Steven Granat**, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, Dell Technologies*

Ha en omfattande incidentresponsplan

När en attack inträffar måste alla viktiga intressenter – i stort sett alla i organisationen och även tredje parter, som leverantörer – veta vad de ska göra. En skriftlig incidentresponsplan bör beskriva en tydlig åtgärdssekvens, råder Shook. En omfattande plan med information om tekniska steg, processteg och kommunikationssteg – allt från omedelbara åtgärder till återställning. Se till att även utarbeta och uppdatera ett skriftligt dokument i tryckt format, eftersom digitala kommunikationssätt kan vara icke-fungerande. ”Man behöver en plan som man bokstavligen kan gå och hämta från hyllan”, säger Granat.

Ha en tydlig kommunikationsstrategi

De flesta organisationer behöver kommunicera med viktiga intressenter och i många fall behöver de uppfylla lagstadgade krav. Skapa olika mallar för både intern och extern kommunikation med systematiska instruktioner gällande vem som ska meddelas i vilken ordning – och när. Planera för att telefon- och mejlsystemen ligger nere.

Implementera en stabil dataskyddsstrategi

Ett viktigt mål med att klara sig igenom en utpressningsvirusattack är att återställa data och att göra det så smärtfritt som möjligt, samtidigt som du undviker att betala lösensumman. En stark dataskyddsstrategi är en viktig del av att uppnå dessa mål, men den måste omfatta både teknik och processer. ”Använd oföränderliga data och cybervalv för att lagra tillräckligt med data som du kan lita på, eller åtminstone som valideringspunkter som gör att du kan återställa systemen”, råder Shook. Att se till att uppgifterna skyddas är det första steget. Du måste också ha rätt personer och processer på plats för att återställa dem. Tredjepartsexperter kan hjälpa till, men de bör tas in redan i planeringsstadiet.

Förutsätt inte en omedelbar återgång till det normala – även om du betalar en lösensumma

Betalning av en lösensumma, som endast bör ses som en sista utväg, garanterar inte att switchen slås på igen direkt. Kom ihåg att det är en brottsling du förhandlar med, och även om du får avkodarnycklarna behöver du en strategi på plats för nyligen återställda data. Till att börja med måste du testa dekrypterade data och bygga om alla system metodiskt. Noggrann uppmärksamhet på ”tänk om”-händelser innan en attack ens äger rum räcker långt för att uppnå tålighet. ”Att förstå de olika applikationerna och beroendena i din tekniska infrastruktur är avgörande för en effektiv återgång till ett stabilt tillstånd. ’Har jag en fungerande återställningskälla och ett återställningsmål?’ ’Har jag data utan kompromisser?’ Det är viktiga saker att tänka på”, säger Granat.

I återställningsfasen måste du också se till att angriparen faktiskt har lämnat dina system. ”Du måste se till att branden i huset är släckt och även ta reda på vad som startade branden i första hand, för utan dessa två avgörande uppgifter är du sårbar för framtida attacker”, säger Shook.

Utbildning och övning är avgörande

En viktig del av cyberelasticitet är omfattande utbildning, som sträcker sig från att se till att medarbetarna tillämpar god cybersäkerhet hela vägen till att rutinmässigt öva på återställningsplanen. ”Du måste ta in rätt personer, genomföra en övning och simulera åtgärder så att alla direkt vet vad de ska göra när en attack inträffar”, säger Shook.

Utpressningsvirus må vara oundvikliga i dagens hotlandskap, men genom planering och genomförande kan du minimera dess inverkan på verksamheten, ekonomin och det goda anseendet. Målet är att återgå till det normala så snabbt och smärtfritt som möjligt.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **dell.com/cybersecuritymonth**

DELL Technologies