ALMA-supporten tipsar!

Vilken februari vi haft

Bitande minusgrader och snö ända nere i ALMASOFTs högkvarter i skånska Veberöd.
Det är ju inte ofta den riktiga vintern hittar hit, så vi har njutit av kylan kan du tro.
Hoppas att du också haft en härligt uppfriskande februari med massor av roliga utomhusaktiviteter.
Men misströsta inte om du börjar bli heligt trött på vintern, för om man tittar riktigt noga bort mot horisonten kan man skönja våren som börjar närma sig så sakteliga.

Och våren kommer med stora nyheter här i ALMASOFTS värld, nämligen något som vi valt att kalla ALMA Cloud.
Ja, du läste rätt! ALMA som web-lösning är ett av våra mest frekventa önskemål, och er vilja är ju vår lag. Eller åtminstone vår största inspiration. Vad vore väl vi utan våra användare? Ingenting!
Därför har vi den senaste tiden jobbat hårt med att kunna lansera en molnbaserad version av ALMA.
Planen är att lansera tjänsten senare i vår, så håll utkik för vidare uppdateringar.

På tal om nyheter, nu har ju version 11.4.2 varit ute ett tag. Har du börjat vänja dig vid hur de nya tänderna i Tandstatus ser ut? Vi har i supporten fått en del synpunkter på att tandgården är väldigt liten nu för tiden. Det behöver den inte vara. I de allra flesta fall kan du enkelt förstora bilden av tandgården genom att bara dra i kanten som separerar tandgården från diagnoserna, samt eventuellt i vänstra kanten mellan tandgården och Patientinformationen.
(Se nedan bild)
På så vis kan du själv anpassa hur stor plats du vill att tandgården ska ta.

Men nog om nyheter för en stund, nu ska vi istället fokusera på det du redan har och hur du håller det säkert. Månadens tema handlar om IT-säkerhet på kliniken.

IT är en ständigt föränderlig värld och cyberattackerna blir alltmer sofistikerade. Att skydda sig kan tyckas vara ett hopplöst omöjligt uppdrag.
Här gäller det främst att vara beväpnad med en rejäl skopa sunt förnuft och att vara källkritisk. Lita inte blint på all epost du får och se till att dina medarbetare har samma kritiska öga och lär sig grunderna i IT-säkerhet. Visste du till exempel att 95% av alla säkerhetsläckor beror på den mänskliga faktorn?
Det är så lätt att öppna fel epost och klicka på fel länk.
De största hoten idag ser inte riktigt likadana ut som de gjorde för bara 5 år sedan, idag är det inte virusen som är de största hoten, utan snarare nätfisket där förövarna fokuserar mycket mer på den enskilde användaren med fokus på att användaren skall luras till att göra något som verkar vara legitimt och korrekt.
Förutom det mest självklara, det vill säga att lösenordskydda datorer och program såsom journalsystemet, finns det även mycket annat man behöver ha i åtanke för att skydda sin data.

Här bjuder vi på några små tips på vägen.

---

1. Ta backup varje dag

Mången katastrof kan man drabbas av i denna datorstyrda värld. Serverkraschar, bränder, vattenläckor, inbrott eller elaka virus för att nämna några.

Så vad gör man egentligen om katastrofen är ett faktum?
Till att börja med ska du se till att vara proaktiv så att du inte står med skägget i brevlådan om olyckan (eller tjuven) skulle vara framme. Det vill säga att du bör ha en plan för vad du ska göra om något skulle drabba din klinik. En bra och säker backup är till exempel A och O för att inte riskera att förlora all din data om något skulle hända. En backup ska tas dagligen och den ska förvaras säkert på annan fysisk plats än där servern finns stationerad.
Den allra tryggaste backuplösningen stavas **eBackup**.

Hur vet du att din backup verkligen fungerar?
Allt för många tar för givet att det bara snurrar på, men så är ju tyvärr inte alltid fallet.
Det är därför viktigt att du skapar rutiner omkring hur du verifierar att din backup fungerar.
Med jämna mellanrum bör du till exempel göra teståterställningar av backupen för att säkerställa att det verkligen går att återställa.
Om du köper en backuptjänst ingår ofta regelbundna teståterläsningar. Men kolla för säkerhets skull alltid upp vad som ingår när du tecknar avtal för en backuptjänst.
Det är även viktigt att du håller ordning på exakt vilken data som backas upp så du inte bara förutsätter att "allt" backas upp per automatik.

---

2. Brandvägg och Antivirus

Många blandar ihop brandvägg och antivirus och tänker att det egentligen är samma sak. Men nej, nog för att de båda har till uppgift att skydda din dator från inkräktare, men de gör detta på olika sätt. Enkelt förklarat kan man säga att Brandväggen är frontlinjen, medan Antivirus fungerar mer som fotsoldater. För ett så komplett skydd som möjligt behöver du alltså båda dessa komponenter.

Brandväggen:
Har till uppgift att filtrera informationen som en dator skickar och tar emot. Den övervakar inkommande och utgående informationspaket, och nekar åtkomst till misstänkta paket. Lite som en vägg alltså; "hit men inte längre". Den kan däremot inte göra något åt eventuell skadlig kod som redan tagit sig in.

Antivirus:
Tar vid där brandväggen slutar, och fokuserar på att hitta och tillintetgöra eventuella hot som tagit sig in i datorn. Programmet skannar datorn regelbundet för virus och kan eliminera eller placera hoten i karantän.

Du är aldrig 100 % säker
Att du har brandvägg och antivirus på datorn innebär tyvärr inte att du har en hundraprocentig garanti för att du går säker från angrepp. Men du kan åtminstone göra så gott du kan.
- Gratis är ju gott men du får oftast vad du betalar för, investera hellre i betalversionerna som ger dig betydligt bättre skydd än gratisversionerna.
- Se till att antivirus och brandvägg alltid är uppdaterade.
- Använd sunt förnuft. Var försiktig med vilka websidor du besöker och vilka mejl du öppnar. Epost-länkar är för övrigt den absolut vanligaste vägen för cyberattacker. Klickar du på fel länk kan inte ens den bästa brandvägg eller antivirus stoppa attacken.

Obs! **Var extra försiktig på din serverdator och undvik om möjligt att använda serverdatorn för att öppna och läsa mejl.**

---

3. Ha Windows Update aktiverat

När ditt Windows uppdateras får du de senaste korrigeringarna och förbättringarna av säkerheten, vilket hjälper din enhet att fungera effektivt och alltid vara skyddad.
Därför är det viktigt att du tillåter att dessa uppdateringar hämtas.

Arbetar du fortfarande på en Windows7-dator? Då är det hög tid att uppgradera. Windows 7 gick i graven för längesedan och supporteras inte längre. Därmed kommer det inte några uppdateringar till Windows 7 vilket i sin tur innebär att du inte har samma funktioner eller samma skydd som med ett modernare operativsystem. arbetspass, som exempelvis i en reception. Då bör datorn undantas från SSO så att respektive användare istället loggar in i ALMA med sitt Windows-lösenord.

Bubblare. Lösenordskydda din data med säkra lösenord

- Spara aldrig lösenord i webbläsaren. Det kan tyckas väldigt bekvämt att ha sina inloggningsuppgifter sparade i webbläsaren så man snabbt och lätt kommer åt sina olika inloggningar. Men ha då i åtanke att om det är snabbt och lätt för dig är det även snabbt och lätt för en potentiell tjuv eller hackare.

- Se till att ha lösenord som är svåra att hacka, ju längre lösenord, desto mer svårhackat.
Och nu behöver du inte börja hyperventilera och få stresseksem, ett långt lösenord behöver inte alls bestå av några hieroglyfer. Tänk fraser istället; lätt för dig att komma ihåg så du slipper skriva upp det någonstans, och dessutom enkelt att ha unika lösenord till alla olika tjänster.
För du har väl inte samma lösenord överallt? Kommer någon åt ditt lösenord på ett ställe så är det i så fall fritt fram överallt. Schackmatt!

Exempel: "Gillar Gula Fräsiga Bilar".
- Google Gillar Gula Fräsiga Bilar
- Facebook Gillar Gula Fräsiga Bilar
- Outlook Gillar Gula Fräsiga Bilar

Antal tecken	Tid att hacka
6	30 sek
7	30 min
8	29 tim
9	71 dygn
10	11 år
11	646 år
12	37 millenier

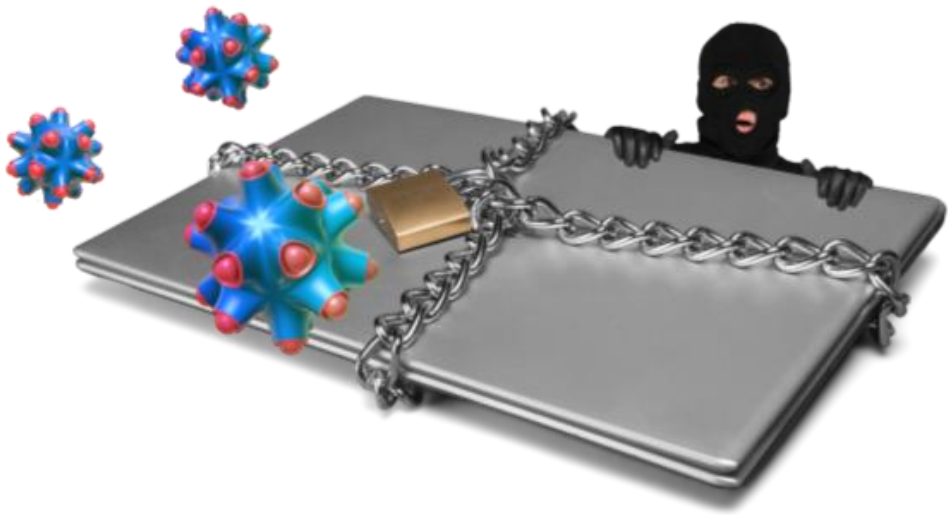
- Extra försiktig ska du vara med din epost. Det är oftast via mejlkontot du kan byta lösenord på olika tjänster eller begära ut nya lösen om du har glömt bort de ursprungliga.
Så ve och fasa, men om någon kapar ditt mejlkonto kan denne person enkelt byta ut lösenordet på alla dina tjänster och faktiskt låsa dig ute från hela din digitala identitet.

- **!** Tänk på att inte förvara journalhandlingar, röntgenbilder och patientuppgifter på datorns skrivbord där de ligger helt oskyddade.

-Logga alltid ut/lås datorn när du lämnar den obevakad. Till exempel när du går på lunch, eller för att göra något i ett annat rum. Man vet aldrig när de långa klåfingrarna kan vara framme.

Inga antivirus eller windowsuppdateringar i världen kan hjälpa dig om du inte även tänker på skalskyddet. Förvara dina datorer på ett säkert sätt. Din server ska du vara extra rädd om då det är här all din data finns. Att förvara datorn fullt synlig genom fönstret är till exempel inte den bästa placeringen. Lås in den på säker plats över natten. Dessutom är larm, säkra lås och brandvarnare kloka investeringar.

Kila nu iväg och byt ut dina lösenord.
Ta hand om dig, och kom ihåg; säkerheten först!



Frostiga vinterhälsningar
//Ditt ALMA-team

Följ gärna almasoft.se på Facebook, Instagram och Linkedin.

Ps: Du vet väl om att du alltid kan gå in på vår hemsida och se Mina sidor, läsa om våra nyheter, produkter och se film. Allt detta hittar du på: www.almasoft.se. Dessutom finns alla våra utgivna nyhetsbrev i utskriftsvänligt pdf-format på vår hemsida: http://www.almasoft.se/tls/support-alma-tls/supporten-tipsar
Tänk på att du måste vara inloggad för att kunna läsa.