Siguria kibernetike në sektorin e arsimit: Si të mbrohen të dhënat nga hakerët

Për shkak të rritjes së përdorimit të mësimit në distancë dhe klasave virtuale, sektori i arsimit ka përjetuar mjaft sulmeve kibernetike.
Sipas Microsoft, arsimi është sektori më i cënueshëm ndaj kërcënimeve si malware, duke përbërë më shumë se 6.8 milionë (mbi 63%) të totalit të raportuar.
"Studentët lindin praktikisht me teknologjinë midis duarve të tyre, por ata nuk kanë informacion për sigurinë" – CISO nga një universitet i madh në Kanada.
Prandaj, siguria kibernetike duhet të jetë pjesë integrale e çdo organizate arsimore. Të gjithë studentët, mësuesit dhe administratorët duhen trajnuar ose ofruar materale ndërgjegjësuese për të kuptuar, zbuluar dhe shmangur kërcënimet kibernetike që mund të hasin në aktivitetet e tyre të përditshme.
Shkollat janë një objektiv ideal, për hakerat, sepse ato janë një minierë ari informacioni personal që rrallëherë mbrohen nga praktikat më të mira të sigurisë kibernetike të cilat i përdorin shumë organizata private.

Mësimet kryesore nga rrjedhet e kaluara të të dhënave (data breach) në arsim

1. Shkollat janë një objektiv kryesor për kriminelët kibernetikë

Sasia e lartë e sulmeve tregon se shkollat duhet të rrisin masat e mbrojtjes së të dhënave ndaj sulmeve kibernetike. Investimi në zgjidhje të tilla të përballueshme si përdorimi i anti-virus-it dhe anti-malware-it, është një domosdoshmëri për mbajtjen e sistemeve të mbrojtura.

2. Stafi duhet të trajnohet më shumë për sigurinë

Edukatorët dhe punonjësit e tjerë në shkolla duhet të informohen rregullisht për rreziqet më të fundit të sigurisë kibernetike për të ditur se si të reagojnë ndaj rrjedhjeve të të dhënave, sulmeve ransomware dhe phishing.

3. Duhet të tregohet kujdes ndaj sulmeve phishing

Kriminelët kibernetikë synojnë institucionet akademike me anë të sulmeve phishing të krijuara për të manipuluar mësuesit që të japin informacione rreth identiteti personal dhe informaciont tatimor të tyre.

Këshilla për sigurinë kibernetike për studentët dhe mësuesit

Për të forcuar sigurinë e informacionit në një mjedis arsimor, studentët, mësuesit dhe punonjësit duhen trajnuar dhe përgatitur rreth sulmeve të ndryshme kibernetike.

Më poshtë listohen disa këshilla kryesore për t'i mbajtur sistemet e shkollës të sigurta:

1. Mbani të përditësuar softuerin

Përditësimi i rregullt i softuerit eliminon dobësitë të cilat përdoren nga hakerat për të nisur sulme ransomware. Rregullimi i softuerit dhe pajisjeve parandalon këdo që të hyjë në sistemet e shkollës pa leje.

2. Instaloni softuer anti-malware dhe anti-virus

Instaloni softuer anti-malware dhe anti-virus, pasi ato bllokojnë malware dhe programe të tjera me qëllim të keq që të mos infektojnë pajisjet e shkollës. Për të forcuar mbrojtjen, zbatoni zgjidhje si përditësime të automatizuara, skanime të viruseve dhe suport ndaj phishing.

3. Zgjidhni fjalëkalime të forta

Zgjidhja e një fjalëkalimi të fortë e bën të vështirë aksesimin e llogarive dhe portaleve institucionale nga kriminelët kibernetikë. Krijimi i fjalëkalimeve duke përdorur shkronja të mëdha dhe të vogla, numra dhe simbole do të ulë mundësitë për një përpjekje të suksesshme hakerimi.

4. Kryeni trajnime ndërgjegjësuese për sigurinë

Sulmet kibernetike po evoluojnë vazhdimisht dhe organizimi i trajnimeve ndërgjegjësuese për sigurinë dhe për phishing për stafin e fakultetit, do t'i ndihmojë ata të fitojnë aftësitë e nevojshme për të zbuluar përpjekjet për phishing dhe të inxhinierisë sociale.

5. Shmangni klikimin në linket e emailit ose hapjen e bashkëngjitjeve

Klikimi në linket e emailit ose hapja e bashkëngjitjeve nga emailat e dërguesve që nuk i njihni është një rrezik sigurie, pasi hapja e një lidhjeje ose një bashkëngjitjeje me qëllim të keq mund të çojë në instalimin e malware. Stafi i fakultetit duhet të kujtohen rregullisht se si të kontrollojnë nëse dërguesi është legjitim përpara se të klikojne mbi ndonjë gjë.