Je geld of een heleboel mensenlevens: de opmars van ransomware

20 december 2019

De artsen en verpleegkundigen van het universiteitsziekenhuis in het Franse Rouen konden onlangs een heel weekend overschakelen op pen en papier: een ransomware-aanval had hun systemen platgelegd. ‘Met gigantische impact: het zorgde voor aanzienlijke vertragingen in het geven van zorg. Naast operationele schade leidde het bovendien tot enorme kosten én imagoschade’, vertelt Lodi Hensen, verantwoordelijk voor het Incident Response Team bij cybersecurity-organisatie Tesorion. ‘Niemand wil naar een ziekenhuis waar je gegevens niet veilig zijn. Het loont dus om te investeren in veiligheid.’

Grote vissen

Zeker als je kijkt naar de trends van het afgelopen jaar. Zo richten cybercriminelen hun pijlen niet langer op individuele organisaties, maar op managed service providers (MSP’s), partijen die IT-diensten aanbieden. Hensen: ‘Met het werken in de cloud besteden ziekenhuizen en zorginstellingen het systeembeheer steeds vaker uit aan een service provider. Gijzelt een cybercrimineel zo’n grote beheerpartij aan, dan is de vangst dus meteen een heel stuk groter en kan hij veel organisaties in één keer afpersen.’

Want om maar meteen een misverstand de wereld uit te helpen: serviceproviders zijn goed in systeembeheer, maar hebben niet altijd de meest actuele *best practices* in cybersecurity.

‘Door misconfiguratie kan er net een poort openstaan in een Remote Desktop Protocol (RDP) dat toegang geeft tot internet’, legt Hensen uit. ‘Het is daarom belangrijk om al voordat je met een serviceprovider in zee gaat, in gesprek te gaan over veiligheid. Hoe alert zijn ze op updates en patches, antivirussoftware en zijn ze gecertificeerd om gevoelige data op te slaan? Wees kritisch en durf daarnaar te vragen.’

Juridisch getouwtrek

Ook is het aan te raden om in clausules vast te leggen wie waar verantwoordelijk en aansprakelijk voor is. ‘Zo is het bijvoorbeeld aan de serviceprovider om de meest recente antivirusscanners te laten draaien, maar aan de organisatie om te zorgen dat die ook aanstaan zodat ze foute bijlagen in e-mails kunnen detecteren’, legt Hensen uit. ‘E-mails en toegang op afstand zijn nog steeds de meest gebruikte manieren om binnen te komen. Door vooraf goede afspraken te maken, voorkom je achteraf juridisch getouwtrek over de rekening. Een data-gijzeling is al vervelend genoeg.’

Vooral omdat de prijzen voor het losgeld stijgen. ‘Dat komt omdat de bedragen worden betaald. Niet betalen bij een ziekenhuis of zorginstelling betekent dat er letterlijk vele mensenlevens in gevaar komen. Ook zijn gezondheidsdata interessant om door te verkopen. Dat kun je je niet veroorloven. Criminelen weten dat de betalingskans groot is en maken daar handig gebruik van. Bovendien bestaan er sinds een paar jaar ook ‘cybercrime-verzekeringen’ die soms ook de kosten van het losgeld dekken. Ook dat verhoogt de betaalkans.’

Systeem als schip

Investeren in veiligheid kan een ransomware-aanval niet voorkomen, maar het criminelen wel lastiger maken. ‘Richt je systeem in als een schip met verschillende compartimenten’, adviseert Lodi Hensen. ‘Door gelaagdheid – bijvoorbeeld niet iedereen toegang geven tot de centrale harde schijf – kun je gevoelige data beter beschermen.’

Verder zijn er geautomatiseerde detectie- en responsoplossingen die meteen reageren als het toch misgaat. ‘Daarnaast zijn er analisten die cyberdreigingen in de gaten houden en daarop acteren. Tot slot helpt mijn team specialisten als het misgaat om te achterhalen wat er is gebeurd en hoe groot de schade is: is het te isoleren of is het hele netwerk geraakt? Maar er komt meer bij kijken dan alleen technologische oplossingen: veel hangt ook af van opvolging en controle. Begin dus met een adviesgesprek om te kijken wat echt bij je organisatie past.’