Smart Working in a Court

Risk Analysis Request

The President of the Tribunal of Bengodi, a mid-sized town in the North of Italy, needs to face the COVID-pandemics. There has been the suggestion to make some Court Clerks (Cancellieri), and now for short Clerks) to work remotely from home with a laptop to limit the travel of people to the office.

The proposal is that people will work with a Windows 10 locked down computer where the officer will log in with user privileges (i.e. no admin) and will use a VPN software by using Juniper Junos Pulse to connect to their office computer which they will be able to manage with the same privileges as they have in the office. It is envisaged to use a remote management software such as TightVNC or TeamSpeak. However, several people have raised concerns that allowing a physical device outside of the Court Offices might compromise the overall security of the system.

As of now the proposal is limited to the Clerks of the Civil and Small Claims Courts[1] (Giudici di Pace). Prosecution and the Criminal Court are excluded from the proposal as they are afraid that this might compromise their investigations.

You should assess how the proposal changes the risk profile of the Tribunal as whole or possibly for some of its department (e.g. the prosecution or the penal or civil courts) or can just be safely carried forward.

The Tribunal has given you a brief guideline to the functioning of the courts from your perspective in terms of operational procedures

a) Each type of courts (Penal Courts, Civil and Small Claims Court, Prosecutor's Offices) has its own President who decides what to do, how to manage the staff (junior judges, court clerks, admin staff members, cleaners etc), and how to spend its budget. Staff are also separated in different offices.
   i)   For your perspective you can consider them separate companies sharing the same large building.
   ii)   Should some service be needed for operation (as any service), it would need to be under the budget of the Courts that must install it.
b) Each case is uniquely assigned to an individual Clerk (except for sick leave etc.) who is responsible for its orderly process and the corresponding digital representation and evolution of the case.
c) There is some level of substitution: a Clerk can take over or review work of other Clerk of the same Court but not of different Courts. So Criminal Courts Clerks should not access Civil Courts.
d) Clerks follow essentially a process that is currently mostly digital and use a specialized software developed specifically for the purpose
   i)   start the case by creating a digital "folder" that is unique to each case;
   ii)   receive a document by a party (or a judge), typically through certified email with digital signatures (physical evidence/documents are close to extinct, for Civil and Small Claims Courts);
   iii) read the document and check that it respects some criteria as a legal document (eventually returning it for fixes to the sending party);
   iv)   file the document into a digital folder in the appropriate classification using the specialized software (such steps may imply a state transition in the judicial process to be recorded in the folder, e.g. from waiting for counter deduction to waiting for court decision, from under debate to adjudicated, etc.);

---

[1] In several places, the Small Claims Courts are less digitized than the Civil Courts so that they might benefit less form smart-working proposal (as people would still need to show in person to submit documents) whereas in others they are at the same level. We do not deal with this distinction and assume we only deal with equally digitized Courts.

v)   notify or remind the appropriate counterparts (and/or the judge) within a set deadline again using certified email with digital signatures;

vi)   take minutes of public hearings (a relative rare event in the process) and file them in the appropriate folder as the other documents

vii)   repeat this procedure until the case is closed which then transformed into a read only document.

e)   The routine of Civil and Small Claims Courts is eventually public: all documents will be eventually released to all counterparties (within a week, a month, or whatever the law says).

f)   Penal Courts and Prosecution have more severe requirements in terms of secrecy to avoid disclosure of investigations, contamination of evidence and possible leaks to the public or to suspects that might lead to slander or criminals taking flight (once a charge is made, the prosecutor's office commits the evidence as available to the counterparty, but not to the public, only the courts have public proceedings)

g)   All judicial proceedings have an essential requirements in terms of meeting deadlines (e.g. issue a notification within x days from the document is received) as otherwise the proceedings may be void (e.g. a prisoner may be released from jail in the Penal Courts, or a debtor may no longer be obliged to pay in Civil Court etc.).

You have asked some clarification of the software they use, and got the following reply

1)   The judicial process software is complex, it would be significantly difficult for anybody who is not a Clerk to mess with it, even to find one's own case as a convict.

2)   Each Clerk has a unique password to access the software and each read or write operation to the folders are logged.

3)   While it would be of course possible for a Clerk to leave one's computer logged on and unattended (e.g. while going to the toilet) a Clerk using the computer of another Clerk would be immediately noticed.

4)   If a Clerk has given the password of another Clerk (for example to do one's a quick favor while doing something else etc) the latter could impersonate the former who would be held responsible for the misdeed.

5)   While several logs are collected (judicial software high level logs, login logs, IP logs etc.,) in case of problems the President of the Court typically reviews the high level logs of the judicial software.

You have asked for the status of the network and software architecture and have been told that

1)   All computers in the tribunal are strictly managed nationally. Judges, Court Clerks and other members have no administrative rights and every software installed on the machine must be vetted. Each staff member has a unique id with password.

2)   No personal system (either mobile or desktop or server) is allowed to connect to the inside network.

3)   There is a global firewall to access the tribunal network but it seems there is not an internal firewall between the different Courts.

4)   As of now all access to the certified email software and the judicial process software are only possible from the computers of the Clerk in the building inside the global firewall,

5)   The tribunal building has three floors and the various functionality of their offices are reported to you in the attached excel file. There is also a very large network of "things" (CCTV camera, etc.)

6)   The network has been segregated in several VLANs with some switches at L2

7)   the VLANs dedicated to external members such as lawyers or the public are in separate VLANs that cannot talk directly to the tribunal VLANs (unless of course going through the Internet)

8)   You have obtained a scan of the network with the recent NESSUS Community edition that is reported in the attached excel file

In terms of operational security you have been told that

1) The different courts officers are distinct so that there is not a single person or physical computer that is shared across Prosecution, Penal, Civil, and Small Claims Courts.
2) Judges have individual offices while Courts Clerks work in offices with typically more people of the same Court. Administrative staff work typically in separate offices from judges and clerks.
3) Court Clerks and Judges may receive visits from the public, e.g. to deposit physical documents, ask for queries, attend court hearings. Visitors are identified and screened for weapons
4) However the administrative services of the Tribunal building are shared among the various offices

You have done some preliminary search and have found out a number of possible cases that raise concerns. Some examples of various problems have been reported below.

In Italy:
1) https://www.vivienna.it/2020/01/17/cresta-al-tribunale-di-enna-arrestato-ex-cancelliere-64enne-condannato-definitivamente-per-peculato-interruzione-di-pubblico-servizio-e-falso/
2) https://www.lastampa.it/imperia-sanremo/2019/05/22/news/corruzione-e-peculato-scatta-il-carcere-per-l-ex-presidente-del-tribunale-boccalatte-1.33703661
3) https://www.rovigooggi.it/n/60053/2017-02-08/cancelliere-condannato-a-due-anni-sospesi-per-una-data
4) https://corrieredelmezzogiorno.corriere.it/napoli/cronaca/20_maggio_11/nola-corruzione-falso-all-ufficio-giudice-pace-arrestati-cancelliere-avvocati-aa3efa8e-935e-11ea-9608-903310728748.shtml
5) https://www.ilgiorno.it/milano/cronaca/talpa-tribunale-truffa-1.5057045
6) https://www.torresette.news/cronaca/2020/05/11/maxi-operazione-dei-carabinieri-arrestati-cancelliere-10-avvocati-e-un-ex-dipendente-comune-di-marigliano
7) https://www.teleclubitalia.it/193864/marigliano-bufera-sugli-uffici-del-giudice-di-pace-arrestati-11-avvocati-e-un-dipendente-del-comune/
8) https://www.lagazzettadelmezzogiorno.it/news/italia/989792/truffa-aste-arrestato-figlio-cancelliere.html
9) https://www.ilgiornale.it/news/milano/grazie-talpa-truffavano-tribunale-1835662.html
10) https://www.edotto.com/articolo/accesso-ai-registri-per-ragioni-estranee-al-servizio-reato-aggravato-per-il-cancelliere

In the UK:
1) http://news.bbc.co.uk/2/hi/uk_news/scotland/edinburgh_and_east/8454771.stm
2) https://www.bbc.com/news/uk-england-london-15689869
3) https://www.theguardian.com/uk/2000/feb/24/8
4) https://www.theguardian.com/uk/2000/mar/29/1

In the USA:
1) https://eu.courier-journal.com/story/news/crime/2017/06/29/court-clerk-accused-stealing-payments-falsifying-records-cover-her-tracks/438725001/
2) https://www.houstonchronicle.com/politics/houston/article/Judge-accused-of-creating-false-court-records-4924254.php
3) https://katv.com/news/local/former-mayflower-court-clerk-accused-of-embezzling-2-million-in-city-funds
4) https://www.nbcmiami.com/news/local/miami-dade-court-clerk-arrested-for-official-misconduct/156732/

5) https://www.theguardian.com/us-news/2015/mar/06/ferguson-court-clerk-racist-emails-fixing-traffic-tickets

Your security background is enough to find out about what a hacker can do with physical access to a device such as USB or Firewire ports etc.) in the recent years so you don't need to be primed on this by the Tribunal.